Bereitstellen von Windows Mobile 6-basierten Geräten mit Microsoft Exchange Server 2007

Einführung

In diesem Leitfaden finden Sie bewährte Methoden und Verfahren zum Implementieren eines Mobile Messaging-Systems mit Microsoft® Windows Mobile® 6-basierten Geräten und Microsoft Exchange Server 2007.

Aufbau des Dokuments

Der Leitfaden ist in zwei Hauptabschnitte unterteilt:

- Der erste Abschnitt, Bereitstellen von Mobile Messaging, enthält eine Übersicht über die neuen Features und die bewährten Methoden zur Bereitstellung; Alternativen und Empfehlungen zur Mobile Messaging-Architektur sowie eine Einführung in die Direct Push-Technologie.
- Der zweite Abschnitt, Bereitstellungsverfahren für Windows Mobile 6 und Exchange Server 2007, beschreibt die Schritte und Verfahren zum Installieren eines Mobile Messaging-Systems. Dazu gehört das Einrichten von Exchange Server 2007, Erstellen einer geschützten Kommunikationsumgebung, Konfigurieren von Microsoft Internet Security and Acceleration (ISA) Server 2006 oder der Firewall eines Drittanbieters sowie die Verwaltung und Konfiguration von mobilen Geräten.

Die in diesem Dokument enthaltenen Informationen stellen die behandelten Themen aus der Sicht der Microsoft Corporation zum Zeitpunkt der Veröffentlichung dar. Da Microsoft auf sich ändernde Marktanforderungen reagieren muss, stellt dies keine Verpflichtung seitens Microsoft dar, und Microsoft kann die Richtigkeit der hier dargelegten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren.
Dieses Whitepaper dient nur zu Informationszwecken. MICROSOFT SCHLIESST FÜR DIESES DOKUMENT JEDE GEWÄHRLEISTUNG AUS, SEI SIE AUSDRÜCKLICH ODER KONKLUDENT.

Die Benutzer/innen sind verpflichtet, sich an alle anwendbaren Urheberrechtsgesetze zu halten. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der Microsoft Corporation kein Teil dieses Dokuments für irgendwelche Zwecke vervielfältigt oder in einem Datenempfangssystem gespeichert oder darin eingelesen bzw. übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen usw.) dies geschieht.

Es ist möglich, dass Microsoft Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von Microsoft eingeräumt.

© 2007 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft, Active Directory, ActiveSync, Internet Explorer, MSDN, Outlook, SharePoint, Windows, Windows Mobile und Windows Server sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Die in diesem Dokument aufgeführten Namen bestehender Unternehmen und Produkte sind möglicherweise Marken der jeweiligen Rechteinhaber.

Inhaltsverzeichnis

BEREITSTELLEN VON MOBILE MESSAGING 1

Voraussetzungen 1
Softwareanforderungen 1
Optionale Komponenten 2
Übersicht über die Bereitstellungssoftware 2
Planungsressourcen 3
NEUE ENTERPRISE-FEATURES IN WINDOWS MOBILE 6 UND EXCHANGE SERVER 2007 4
Neue Features: Windows Mobile 6-basierte Geräte 4
Neue Features: Exchange Server 2007 6
BEWÄHRTE METHODEN FÜR DIE BEREITSTELLUNG VON MOBILE MESSAGING 11
Netzwerkkonfiguration 11
Sicherheitsfeatures: Authentifizierung und Zertifizierung 13
SZENARIEN DER NETZWERKARCHITEKTUR 15
Bereitstellungsoptionen 15
Authentifizierung in ISA Server 2006 21
GRUNDLEGENDES ZU DIRECT PUSH 23
Direct Push-Technologie 23

BEREITSTELLUNGSVERFAHREN ZU WINDOWS MOBILE 6 UND EXCHANGE SERVER 2007 29

SCHRITT 1: INSTALLIEREN VON EXCHANGE SERVER 2007 MIT DER CLIENT ACCESS-SERVERFUNKTION 30
SCHRITT 2: AKTUALISIEREN DER SERVER MIT SICHERHEITSPATCHES 33
SCHRITT 3: SCHÜTZEN DER KOMMUNIKATION ZWISCHEN EXCHANGE SERVER 2007 UND WINDOWS MOBILE 6-BASIERTEN GERÄTEN 34
Bereitstellen von SSL zum Verschlüsseln des Messagingverkehrs 34
Aktivieren von SSL für die Standardwebsite 46
Konfigurieren der Standardauthentifizierung 47
Schützen von IIS durch eine Verringerung potenzieller Angriffsflächen 50
SCHRITT 4: INSTALLIEREN UND KONFIGURIEREN VON ISA SERVER 2006 ODER EINER ANDEREN FIREWALL 51
Verfahren 51
Installieren von ISA Server 2006 52
Installieren eines Serverzertifikats auf dem Computer mit ISA Server 52
Aktualisieren von öffentlichen DNS 55
Erstellen der Exchange ActiveSync-Webveröffentlichungsregel 56
Konfigurieren von ISA Server 2006 für die LDAP-Authentifizierung 64
Festlegen des Zeitlimits für Leerlaufsitzungen für Firewalls und Netzwerkgeräte auf 1800 Sekunden 66
Testen der Exchange-Veröffentlichungsregel 67
SCHRITT 5: KONFIGURIEREN UND VERWALTEN DES ZUGRIFFS ÜBER MOBILE GERÄTE AUF DEN EXCHANGE-SERVER 68
Erstellen von Exchange ActiveSync-Postfachrichtlinien 68
Konfigurieren der Sicherheitseinstellungen für mobile Geräte mit Postfachrichtlinien 70
Anwenden einer Postfachrichtlinie auf einen Benutzer 71
Ausführen einer Remotegerätzurücksetzung 72
Deaktivieren von Exchange ActiveSync 75
SCHRITT 6: ZERTIFIKATREGISTRIERUNG UND GERÄTEPROVISIONING 77
Zertifikate auf Windows Mobile-basierten Geräten 77

Standardauthentifizierung *80*
Zertifikatbasierte Authentifizierung *80*
Verwalten von Gerätezertifikaten *81*
Windows Mobile-Sicherheitsrichtlinien und Geräteprovisioning *85*
SCHRITT 7: VERWALTEN UND KONFIGURIEREN VON WINDOWS MOBILE 6-BASIERTEN GERÄTEN 87
Einrichten einer Verbindung zwischen mobilen Geräten und dem Exchange-Server *87*

Bereitstellen von Mobile Messaging

Dieser Leitfaden wurde für IT-Profis entwickelt, die für die Planung und Bereitstellung eines Mobile Messaging-Systems mit Microsoft® Exchange Server 2007 und Windows Mobile 6-basierten Geräten verantwortlich sind.

Voraussetzungen

Der Leitfaden setzt allgemeine Kenntnisse in Folgendem voraus: Bereitstellung und Verwaltung von Microsoft Exchange Server 2007, Microsoft Office Outlook® Web Access, Exchange ActiveSync®, HTTP (Hypertext Transfer Protocol) und in Konzepten von Microsoft Internetinformationsdienste (Internet Information Services, IIS).

Hinweis:

> Exchange Server 2007 ermöglicht erstmalig die Bereitstellung verteilter Serverfunktionen und bietet eine zusätzliche Funktionalität, die in früheren Versionen von Microsoft Exchange nicht verfügbar war. Lesen Sie vor der Installation Ihrer Mobile Messaging-Lösung mit Windows Mobile 6 und Exchange Server 2007 auf jeden Fall zuerst die technische Dokumentation zu Microsoft Exchange Server 2007 in der Microsoft TechNet-Bibliothek.

Weitere Informationen zur Funktionalität von Exchange Server 2007, Serverfunktion, Architektur und Planung sowie zu Exchange ActiveSync finden Sie im Abschnitt zu den ersten Schritten zu Microsoft Exchange Server 2007 unter http://go.microsoft.com/fwlink/?LinkID=87058&clcid=0x409 (möglicherweise in englischer Sprache).

Softwareanforderungen

Die folgende Tabelle zeigt, welche Betriebssysteme und Anwendungen für eine einzelne Bereitstellung von Exchange Server 2007 erforderlich sind.

Bereich	Softwareanforderungen
Active Directory® Server Lightweight Directory Access Protocol (LDAP)	• Microsoft Windows Server® 2003 oder Microsoft Windows Server 2000 (Windows Server 2003 mit Service Pack 1 (SP1) wird empfohlen)
Exchange Server	• Microsoft Exchange Server 2007 • 64-Bit-Version von Windows Server 2003 oder Windows Server 2003 R2 • Client Access-Serverfunktion (installiert) • Microsoft Windows Server 2003 mit Service Pack 1 (SP1) • Internetinformationsdienste (IIS) 6.0
Mobile Geräte	• Windows Mobile 6-basierte Geräte

Bereitstellen von Windows Mobile 6-basierten Geräten mit Microsoft Exchange Server 2007

Hinweis:

- Für die Installation von Microsoft Exchange Server 2007 sind eine 64-Bit-Hardware und ein 64-Bit-Betriebssystem Voraussetzung. Auf diese Weise können die höheren Arbeitsspeicher-, Speicher- und erweiterten Sicherheitsanforderungen kostengünstig unterstützt werden. Bei umfangreichen Exchange-Bereitstellungen, bei denen sich der Clientzugriffsserver auf einem anderen Computer befindet als die Exchange Mailbox-Serverfunktion, wird dringend empfohlen, Exchange Server 2007 nicht auf einem Domänencontroller, sondern auf einem Mitgliedsserver bereitzustellen.
- Weitere Informationen zu den Hardware- und Softwarevoraussetzungen für Exchange Server 2007 finden Sie im Thema zur Vorbereitung auf die Bereitstellung von Exchange 2007 im Abschnitt zur Bereitstellung unter http://go.microsoft.com/fwlink/?LinkID=87058&clcid=0x409 (möglicherweise in englischer Sprache).

Optionale Komponenten

- Sie können die folgenden optionalen Komponenten für Sicherheitsfeatures und zur Geräteverwaltung implementieren:
- Microsoft Internet Security and Acceleration Server 2006
- Windows-Zertifizierungsstelle
- RSA Authentication Manager 6.0 von RSA Security
- RSA Authentication Agent für Microsoft Windows von RSA Security
- RSA SecurID Authenticator von RSA Security

Weitere Informationen zu Gruppenrichtlinien finden Sie weiter unten in diesem Dokument unter Szenarien der Netzwerkarchitektur.

Übersicht über die Bereitstellungssoftware

Da sich die Netzwerkinfrastrukturen und Sicherheitsrichtlinien der Unternehmen unterscheiden, gibt es keinen einheitlichen Bereitstellungsprozess für die Mobile Messaging-Installation. Es gibt sowohl erforderliche als auch empfohlene Schritte zur Bereitstellung einer Messaginglösung mit Microsoft Exchange Server 2007 und Windows Mobile 6-basierten Geräten.
Die Bereitstellung kann in sieben Schritten erfolgen:

Schritt 1: Installieren von Exchange Server 2007 mit der Client Access-Serverfunktion

Schritt 2: Aktualisieren der Server mit Sicherheitspatches

Schritt 3: Schützen der Kommunikation zwischen Exchange Server 2007 und Windows Mobile 6-basierten Geräten

Schritt 4: Installieren und Konfigurieren von ISA Server 2006 oder einer anderen Firewall

Schritt 5: Konfigurieren und Verwalten des Zugriffs über mobile Geräte auf den Exchange-Server

Schritt 6: Zertifikatregistrierung und Geräteprovisioning

Schritt 7: Verwalten und Konfigurieren von Windows Mobile 6-basierten Geräten

Planungsressourcen

Die folgenden Websites und technischen Artikel von Microsoft enthalten Hintergrundinformationen, die bei der Planung und Bereitstellung Ihrer Mobile Messaging-Lösung hilfreich sein können:

Exchange Server 2007/Windows Server 2003/ISA Server 2006/IIS 6.0
Bereitstellungshandbuch für Exchange Server 2007 http://go.microsoft.com/fwlink/?LinkID=87058&clcid=0x409 (möglicherweise in englischer Sprache)
Bereitstellungshandbuch für Windows Server 2003 http://go.microsoft.com/fwlink/?LinkId=62630 (möglicherweise in englischer Sprache)
Bereitstellen von Exchange Server 2007 mit ISA Server 2006 http://go.microsoft.com/fwlink/?LinkID=87060&clcid=0x409 (möglicherweise in englischer Sprache)
Windows Server 2003 Technische Referenz http://go.microsoft.com/fwlink/?LinkId=62631 (möglicherweise in englischer Sprache)
IIS 6.0 Bereitstellungshandbuch (IIS 6.0) http://go.microsoft.com/fwlink/?LinkId=62632 (möglicherweise in englischer Sprache)
Microsoft Exchange Server TechCenter http://go.microsoft.com/fwlink/?LinkId=62633 (möglicherweise in englischer Sprache)
Supporting Windows Mobile Powered Devices Within the Enterprise: Corporate Guidelines for Each Stage of the Device's Lifecycle (Whitepaper) http://go.microsoft.com/fwlink/?LinkId=62635

Neue Enterprise-Features in Windows Mobile 6 und Exchange Server 2007

Dieser Abschnitt enthält Informationen zur neuen Funktionalität in Windows Mobile 6 und Microsoft Exchange Server 2007. Features, die nicht direkt mit der Bereitstellung von Mobile Messaging zusammenhängen, werden nicht behandelt. Sie finden hier jedoch Links zu den entsprechenden Themen.

Neue Features: Windows Mobile 6-basierte Geräte

Windows Mobile 6 ist die nächste Hauptversion für Windows Mobile-basierte Geräte nach Windows Mobile 5.0. Folgende Funktionen sind neu in der Windows Mobile 6-Software:

Erweiterte geräteeigene Verwaltungs- und Sicherheitsfeatures

Verbesserte Zertifikatregistrierung und Verwaltung

Exchange-Suche für E-Mail

Dokumentzugriff auf Microsoft SharePoint®- und Windows-Dateifreigaben

HTML-Unterstützung in E-Mail

Erweiterte geräteeigene Verwaltung und Sicherheit

Windows Mobile 6-basierte Geräte verfügen über eine höhere Interoperabilität mit Exchange Server 2007. Die Windows Mobile 6-Softwarearchitektur bietet bessere Geräteverwaltungs- und Sicherheitsfunktionen, eine engere Integration in Exchange Server 2007 und weitere Produktivitätstools. Unternehmen können dadurch Windows Mobile-Lösungen noch effizienter bereitstellen, verwalten und sichern als zuvor.

Eine erweiterte Flexibilität der Richtlinienverwaltung sowie verbesserte Gerätesteuerungs- und Sicherheitsfeatures steigern die Leistung der integrierten mobilen Unternehmenslösungen. Diese neuen Features und Gerätefunktionen vereinfachen das Erstellen von Branchenanwendungen (Line-of-Business, LOB). Windows Mobile 6 kann den höchsten Standard für die Entwicklung und Bereitstellung von LOB-Anwendungen bieten.

Verbesserte Zertifikatregistrierung und Verwaltung

Windows Mobile 6 enthält eine geräteseitige Registrierfunktion, die sich im ROM aller Windows Mobile-basierten Geräte befindet. Darüber hinaus ermöglicht eine Desktopregistrierfunktion von ActiveSync 4.5 dem Benutzer, die Registrierung mithilfe einer Desktopbenutzeroberfläche zu konfigurieren und auszuführen. Die Funktionalität beinhaltet das Erstellen der Einstellungen für die Zertifikatregistrierung und die Möglichkeit, die Desktopdomänenanmeldung zur Gerätezertifikatregistrierung zu verwenden. Die Desktopzertifikatregistrierung ermöglicht dem Benutzer mithilfe der Desktopauthentifizierung per Smartcard, bei der Domäne ein Zertifikat in seinem Gerät zu registrieren. Ein Smartcardleser oder Smartcardsoftware ist dabei im Gerät nicht erforderlich. Erweiterte Sicherheitsfeatures in Windows Mobile 6 unterstützen eine anwendungsgesteuerte Registrierung, unterstützen Bereitstellungen, die eine kennwortlose Authentifizierung (Smartcard) erfordern, und bieten die Möglichkeit, abgelaufene Zertifikate zu erneuern.

Hierzu gehören folgende Features:

- Eine zertifikatbasierte Authentifizierung kann die herkömmliche Benutzername-/Kennwort-Authentifizierung ersetzen.
- Eine flexible Plattformzertifikatregistrierung kann im Gerät konfiguriert werden.
- Anwendungen können programmgesteuert in den Zertifikatregistrierungsprozess eingreifen, um die Registrierung einzuleiten.

- Die Zertifikaterneuerung wird unterstützt.
- Zusätzliche Zertifikate können im Gerät installiert werden, ohne dass eine CAB-Datei erstellt werden muss.

Exchange-Suche für E-Mail

Bei der Exchange-Suche für E-Mail können Benutzer von Windows Mobile 6-basierten Geräten ihre Microsoft Exchange-Postfächer nach Elementen durchsuchen, die bestimmten Kriterien entsprechen. Die Suchergebnisse werden heruntergeladen und in einem Ordner angezeigt. Die Möglichkeit, E-Mail im Exchange-Speicher des Benutzers zu durchsuchen, ist ein leistungsstarkes Feature. Damit können Benutzer auf wichtige Informationen in ihrem Exchange-Postfach zugreifen, wenn sie sich nicht an einem Schreibtisch aufhalten. Benutzer erhalten auch unterwegs stets die Informationen, die sie brauchen.
Die folgenden neuen Features werden unterstützt:

- Informationen in E-Mail-Nachrichten, die sich nicht auf dem mobilen Gerät befinden, können gesucht werden.
- Suchergebnisse werden in einem Standardnachrichtenordner angezeigt.
- Der Benutzer kann Felder, Ordner und Datumsbereiche angeben, die durchsucht werden sollen.
- Der Benutzer kann Nachrichtentext und Anlagen aus den Suchergebnissen abrufen.
- Die Ergebnisse bleiben bis zur nächsten Suche oder bis sie vom Benutzer gelöscht werden im Suchordner.
- Der Benutzer sieht die maximale Anzahl der verfügbaren Suchergebnisse.

Dokumentzugriff auf SharePoint- und Windows-Dateifreigaben

Der SharePoint-Dokumentzugriff ermöglicht es authentifizierten mobilen Benutzern, die in HTML-Nachrichten eingebetteten Links auszuwählen und Dokumente zu öffnen, die auf SharePoint-Servern gespeichert sind. Dasselbe gilt auch für freigegebene UNC-Dokumente (Universal Naming Convention). Dadurch müssen die Dateien der E-Mail-Nachricht nicht als Anlage hinzugefügt werden, was Bandbreiten- und Speicherkapazitäten spart. Außerdem stellt diese Vorgehensweise sicher, dass der Empfänger die neueste Version eines Dokuments erhält.

Mobile Benutzer können außerhalb der Unternehmensfirewall in der Regel nicht auf Dokumente zugreifen. Die Verwendung von Microsoft Exchange Server 2007 als Proxy oder Redirector für das Dokument löst dieses Problem. Dabei können HTML-Nachrichten wie bei herkömmlichen Anlagen Links zu SharePoint-Dokumenten enthalten.

Hinweis:

Windows Mobile 6 ermöglicht einen schreibgeschützten Zugriff auf Elemente, die in SharePoint- und in UNC-Freigaben gespeichert sind.

HTML-Unterstützung in E-Mail

HTML-E-Mail ist eine Erweiterung von Microsoft Outlook Mobile®, die Benutzern das Empfangen, Anzeigen, Verfassen und Senden von E-Mail-Nachrichten im HTML-Format ermöglicht. Die folgenden Übertragungsarten werden unterstützt: ActiveSync, POP, IMAP und Exchange Server 2007. Zur HTML-Funktionalität gehören Listen, Tabellen, Hyperlinks, formatierter Text und Inlinebilder.
Die Windows Mobile 6-Software enthält die folgenden neuen HTML-Funktionen:

- Mit Exchange Server 2007 synchronisierte E-Mail-Nachrichten zeigen das HTML-Originalformat an.
- Intelligente HTML-Antworten, eine intelligente Inlineweiterleitung sowie das Verfassen und Abrufen von E-Mail werden unterstützt.

- Weitergeleitete E-Mail-Nachrichten werden nun wie bei der Desktopversion von Outlook inline dargestellt.
- In den E-Mail-Nachrichten werden Inlinehyperlinks zu Webinhalten beibehalten.
- Richtlinien und Benutzeroptionen: Das HTML-Aufkommen pro Konto wird über Konfigurationsanbieter und Benutzeroptionen gesteuert.

Hinweis:

Abgesehen von den hier aufgeführten Funktionen verfügt Windows Mobile 6 noch über weitere neue Features, einschließlich Gerätesperrung, erweiterter PIN-Sicherheit und Speicherkartenverschlüsselung. Weitere Informationen zu neuen Features und Funktionen von Windows Mobile finden Sie im Handbuch zu Windows Mobile 6 unter http://go.microsoft.com/fwlink/?LinkID=88410&clcid=0x409 (möglicherweise in englischer Sprache).

Neue Features: Exchange Server 2007

Microsoft Exchange Server 2007 bietet verschiedene neue Features, die die Leistung Ihrer Windows Mobile 6-Messaginglösung erhöhen und die Verwaltung vereinfachen. Nahezu alle Verwaltungsaufgaben erfolgen über die Exchange-Verwaltungskonsole. Zusätzliche Tools zur Geräteverwaltung sind somit überflüssig. Die folgenden Features sind neu in Exchange Server:

- Neue Exchange Server 2007 ActiveSync-Funktionalität
- Exchange ActiveSync-Postfachrichtlinien
- Verteilte Serverfunktionen
- Exchange-Verwaltungskonsole
- Microsoft Exchange Server 2007 Management Pack für Microsoft Operations Manager (MOM) 2005

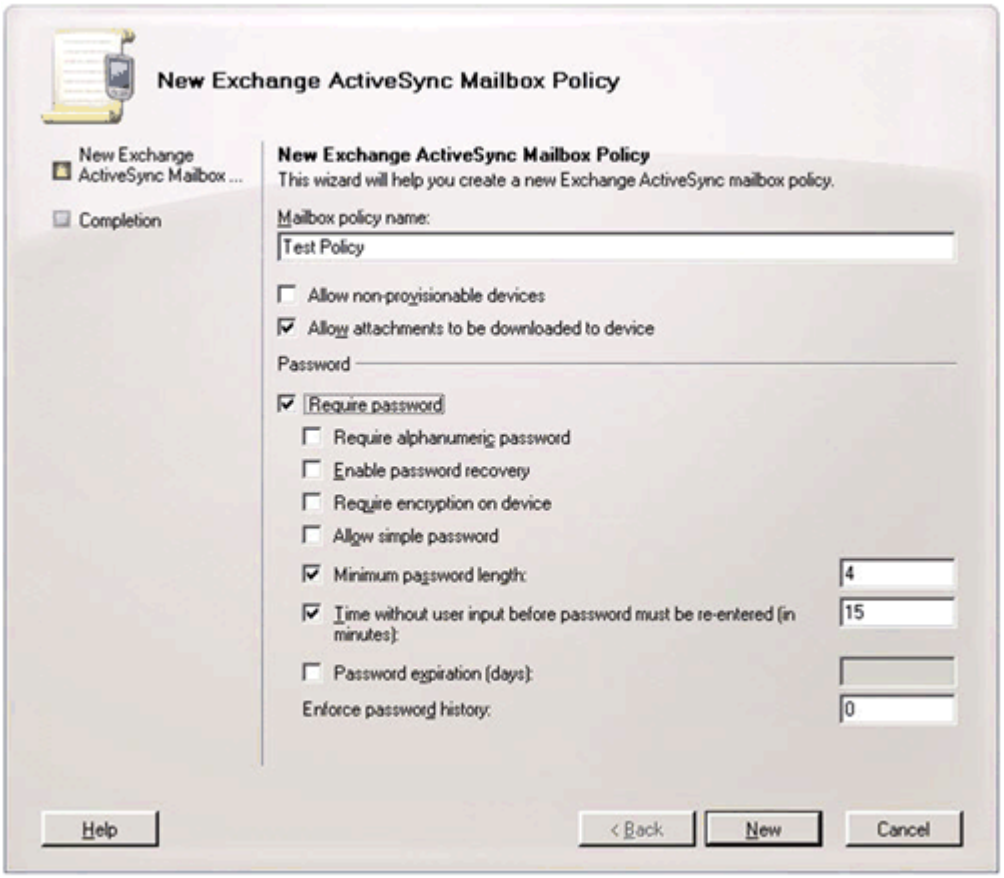
Neue Exchange Server 2007 ActiveSync-Funktionalität

Exchange ActiveSync wird bei installierter Client Access-Serverfunktion standardmäßig für Exchange Server 2007 aktiviert. Exchange ActiveSync ist in Exchange Server 2007 verbessert worden. Folgende neue ActiveSync-Features sind verfügbar:

- Unterstützung für HTML-Nachrichten
- Unterstützung für Nachverfolgungskennzeichnungen
- Unterstützung für den schnellen Nachrichtenabruf
- Informationen zu Besprechungsteilnehmern
- Verbesserte Exchange-Suche
- Zugriff auf Windows SharePoint Services- und UNC-Dokumente
- Zurücksetzen der PIN
- Erweiterte Features zur Gerätesicherheit durch Kennwortrichtlinien
- Unterstützung für die Abwesenheitskonfiguration

Exchange ActiveSync-Postfachrichtlinien

Mithilfe von Exchange ActiveSync-Postfachrichtlinien kann der Administrator einer Benutzergruppe eine Reihe allgemeiner Richtlinien und Sicherheitseinstellungen zuweisen. Mit Exchange Server 2007 sind verschiedene zusätzliche Richtlinien eingeführt worden, die eine umfassendere Verwaltung der Mobile Messaging-Umgebung ermöglichen.



Über die Exchange-Verwaltungskonsole können die folgenden Richtlinienoptionen für Mobile Messaging festgelegt werden:

Sicherheitsoption	Beschreibung
Alphanumerisches Kennwort anfordern	Verwenden Sie diese Option, wenn die Benutzer Kennwörter aus Zahlen und Buchstaben verwenden sollen. Diese Option ist nicht standardmäßig aktiviert.
Kennwortwiederherstellung aktivieren	Der Administrator kann mithilfe der Exchange-Verwaltungskonsole ein Wiederherstellungskennwort abrufen.
Verschlüsselung auf dem Gerät anfordern	Verlangt für Smartcards eine Verschlüsselung auf dem Gerät.
Einfaches Kennwort zulassen	Aktiviert oder deaktiviert die Möglichkeit, ein einfaches Kennwort wie „1234“ zu verwenden.
Minimale Kennwortlänge	Gibt die minimale Kennwortlänge an.

Sicherheitsoption	Beschreibung
Zeitraum ohne Benutzereingabe, bis das Kennwort erneut eingegeben werden muss	Gibt an, ob sich der Benutzer nach Ablauf der angegebenen Minuten, während denen das Gerät nicht verwendet wurde, anmelden muss. Diese Option ist nicht standardmäßig aktiviert. Bei Aktivierung beträgt die Standardeinstellung 5 Minuten.
Kennwortablauf	Der Administrator kann den Zeitraum konfigurieren, nach dem ein Gerätekennwort geändert werden muss.
Das Herunterladen von Anlagen auf das Gerät zulassen	Ermöglicht das Herunterladen von Anlagen auf das mobile Gerät.
Nicht bereitstellbare Geräte zulassen	Lässt die Verbindung älterer Geräte mit Exchange Server 2007 über ActiveSync zu.

Eine detaillierte Übersicht über die Postfachrichtlinien von Exchange Server 2007 finden Sie im Abschnitt zu den ActiveSync-Postfachrichtlinien unter http://go.microsoft.com/fwlink/?LinkID=87062&clcid=0x409 (möglicherweise in englischer Sprache).

Verteilte Serverfunktionen

Die Bereitstellung von Exchange Server 2007 kann als Standardinstallation oder benutzerdefiniert erfolgen. Bei einer Standardinstallation werden einer einzelnen Plattform mehrere Serverkomponenten (Serverfunktionen) hinzugefügt.

Eine Serverfunktion ist eine Einheit, mit der Features und Komponenten, die zum Ausführen bestimmter Funktionen in der Messagingumgebung erforderlich sind, logisch zusammengefasst werden. Die Serverfunktion dient als Server, der zur automatischen Bereitstellung bestimmter Features ausgeführt werden kann. Serverfunktionen sind die vorrangigen Bereitstellungseinheiten und ermöglichen dem Administrator eine einfache Auswahl der Features, die auf einem Exchange-Server installiert werden sollen. Logisch in Serverfunktionen gruppierte Features bieten folgende Vorteile:

- Die Angriffsfläche eines Exchange-Servers wird verringert. Der Administrator kann weitere Back-End-Server hinzufügen, ohne den Betrieb der Clientzugriffsserver zu unterbrechen und ohne dass von außerhalb des Unternehmens-LANs auf diese Server zugegriffen werden kann.
- Die Installation ist einfach, und die Server können voll und ganz den Geschäftszielen und -anforderungen entsprechend angepasst werden.
- Die Serverleistung kann sich erhöhen, da die Gesamtauslastung (CPU- und Speichernutzung) auf zusätzliche Serverplattformen verteilt werden kann.

In einer Mobile Messaging-Bereitstellung sind die folgenden Exchange Server 2007-Serverfunktionen entscheidend:

- Client Access-Serverfunktion (Clientzugriffsserver) - Diese Funktion unterstützt Microsoft Exchange ActiveSync-Clientanwendungen sowie die Protokolle POP3 (Post Office Protocol Version 3) und IMAP4 (Internet Message Access Protocol Version 4rev1). Dabei handelt es sich um die vorrangige Serverkomponente des Mobile Messaging-Systems. Der Clientzugriffsserver dient in einer Topologie mit verteilten Funktionen als Front-End-Server für den Postfachserver (Back-End).
- Mailbox-Serverfunktion (Postfachserver) - Dieser Back-End-Server stellt Postfächer und öffentliche Ordner bereit.

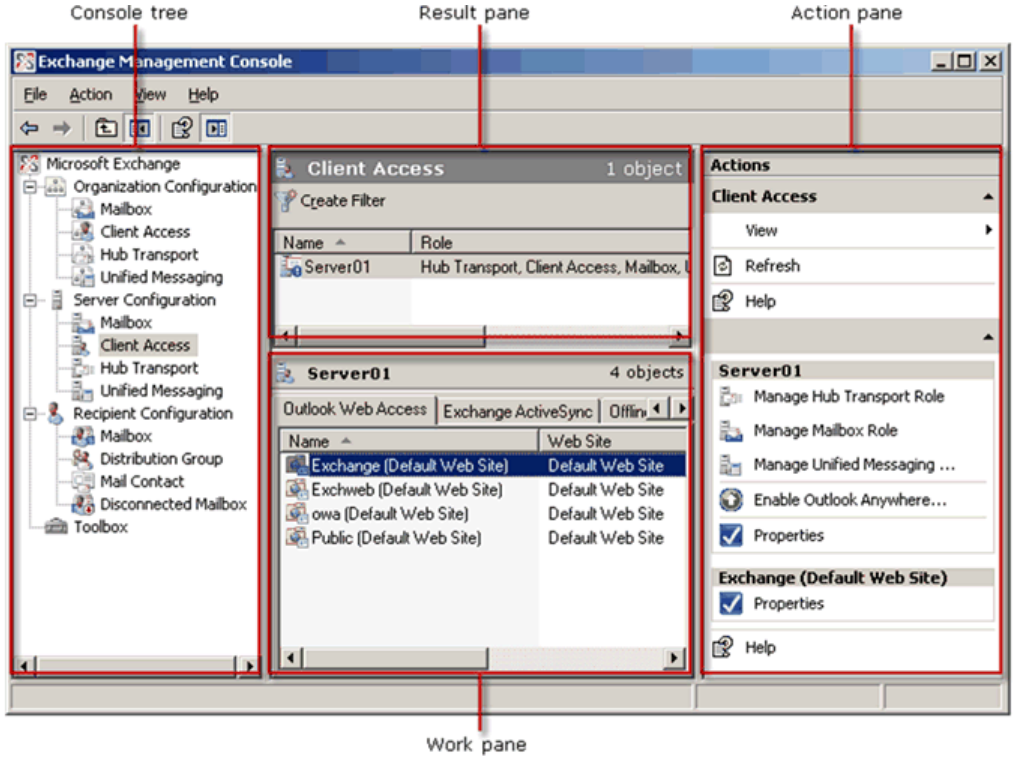
Hinweis:

Zu den weiteren, hier nicht oder nur kurz erwähnten Serverfunktionen gehören Edge-Transport-, Hub-Transport und Unified Messaging. Die Client Access-Serverfunktion beinhaltet die ActiveSync-Kommunikation mit einem Windows Mobile-basierten Gerät. Sie ist die entscheidende Komponente einer Mobile Messaging-Bereitstellung. (Siehe Szenarien der Netzwerkarchitektur.)

Weitere Informationen zu Microsoft Exchange 2007-Serverfunktionen finden Sie im Leitfaden zu den Serverfunktionen in Microsoft Exchange Server 2007 unter http://go.microsoft.com/fwlink/?LinkID=87058&clcid=0x409 (möglicherweise in englischer Sprache).

Exchange-Verwaltungskonsole – Übersicht

In Exchange Server 2007 ersetzt die Exchange-Verwaltungskonsole den Exchange-System-Manager von Exchange Server 2003. Mit der Exchange-Verwaltungskonsole können Sie alle Server, Empfänger und Organisationskomponenten Ihrer IT-Infrastruktur verwalten.



Ein Aktionsbereich zeigt dem Administrator nun die Aktionen an, die für die in der Konsolenstruktur oder dem Ergebnisbereich ausgewählten Elemente verfügbar sind. In Bezug auf Mobile Messaging heißt das z. B., dass im Aktionsbereich neue Postfachrichtlinien erstellt oder Daten eines mobilen Geräts gelöscht werden können.

Hinweis:

Das Exchange ActiveSync Mobile Administration Web Tool ist in Exchange Server 2007 nicht mehr verfügbar. Das Webtool ermöglicht Administratoren, die remote Bereinigung von verlorenen, gestohlenen oder auf andere Weise gefährdeten mobilen Geräten in einer Exchange Server 2003-Umgebung durchzuführen. Diese Funktionalität ist der Exchange-Verwaltungskonsole hinzugefügt worden. Somit sind nun alle Verwaltungsfunktionen in einer einzigen Benutzeroberfläche zusammengefasst.

Microsoft Exchange Server 2007 Management Pack für Microsoft Operations Manager (MOM) 2005

Das Exchange Server 2007 Management Pack enthält Regeln und Skripts zur Überwachung und Berichterstellung hinsichtlich der Leistung, Verfügbarkeit und Zuverlässigkeit aller Exchange 2007-Serverfunktionen: Mailbox, Client Access, Hub-Transport, Edge-Transport und Unified Messaging. Die Themen zum Exchange Server 2007 Management Pack für MOM 2005 erläutern, wie die Messagingressourcen überwacht und verwaltet werden. Sie finden die speziellen Themen online im Abschnitt zum Überwachen von Exchange 2007 mit Microsoft Operations Manager 2005 SP1 unter http://go.microsoft.com/fwlink/?LinkID=87063&clcid=0x409 (möglicherweise in englischer Sprache).

MOM 2005 und Microsoft Exchange Server 2007 sind für das Microsoft Exchange Server 2007 Management Pack erforderlich.

Bewährte Methoden für die Bereitstellung von Mobile Messaging

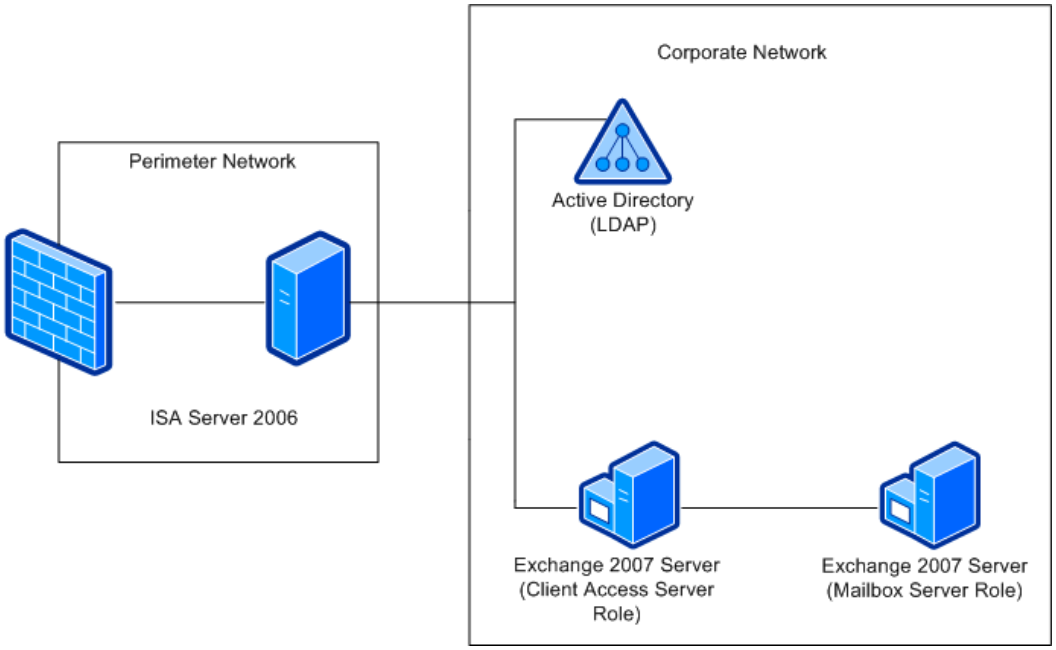
In diesem Abschnitt werden die bewährten Methoden für die Bereitstellung des Mobile Messaging von Microsoft erläutert, sodass die Sicherheitsanforderungen Ihrer Organisation erfüllt werden können.

Netzwerkkonfiguration

Es gibt einige bewährte Methoden für die Netzwerkkonfiguration, mit denen Sie unabhängig von der von Ihnen implementierten Konfiguration eine leistungsfähigere Mobile Messaging-Lösung erhalten.

Verteilte Serverfunktionen in Exchange 2007

Zu den Änderungen in Exchange Server 2007 gehört das Erstellen von Exchange-Serverfunktionen, mit denen Sie auswählen können, welche Exchange-Komponenten auf den einzelnen Servern installiert werden. Exchange ActiveSync ist die Exchange-Komponente für die Kommunikation mit dem mobilen Gerät. Für ActiveSync wird die Exchange-Serverfunktion Client Access verwendet. Eine bewährte Methode ist hierbei, dass die Client Access-Serverfunktion einer Domäne angehört und sich am selben Active Directory-Standort befindet wie die Exchange Mailbox-Serverfunktion. Eine weitere bewährte Methode besteht darin, den gesamten Internetverkehr über einen Reverseproxy oder eine Firewall, wie z. B. ISA 2006, zu leiten. ISA 2006 besitzt eine integrierte Sicherheitsfunktionalität, z. B. SSL-Bridging, Benutzerauthentifizierung und Paketprüfung.



In diesem Netzwerkdiagramm fungiert der Clientzugriffsserver (Client Access-Serverfunktion), der die Kommunikation mit Exchange Server 2007 ActiveSync übernimmt, als Front-End für das Back-End Postfachserver (Mailbox-Serverfunktion). ISA Server 2006 befindet sich im Perimeternetzwerk und filtert eingehende Anforderungen an den Clientzugriffsserver. Ein Vorteil einer verteilten Architektur besteht darin, dass die CPU- und Speichernutzung eines einzelnen Servers entlastet wird.

Je nach Größe der Organisation kann diese Topologie dabei helfen, die Gesamtleistung des Mobile Messaging-Systems zu verbessern. Bei weniger umfangreichen Implementierungen können die Client Access- und die Mailbox-Funktion auf demselben Computer bereitgestellt werden.

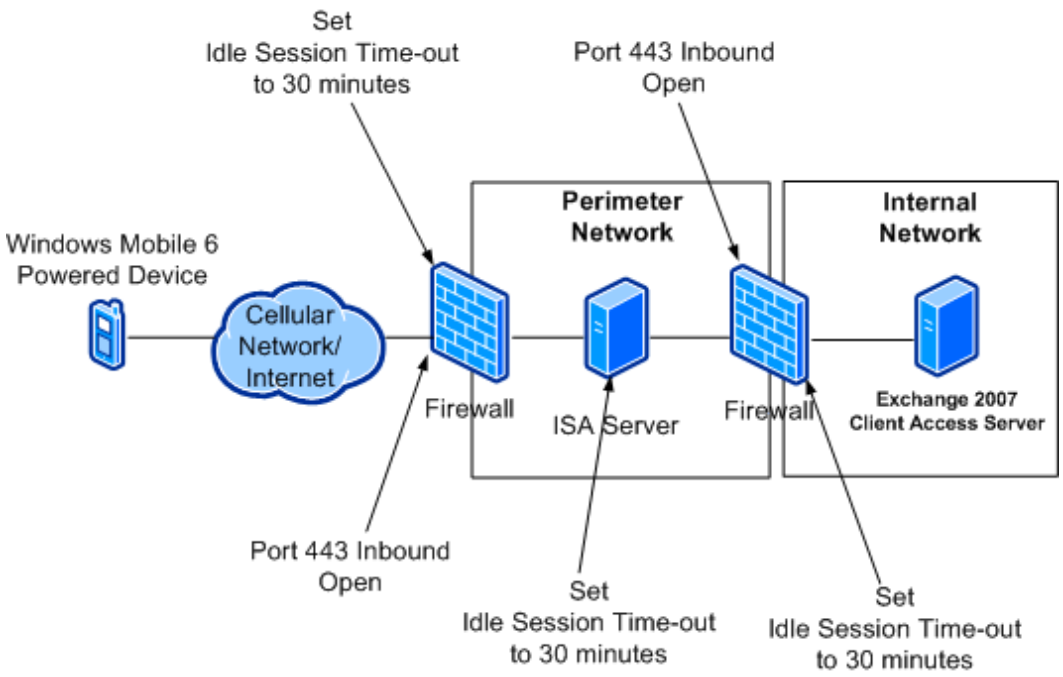
Weitere Informationen zu Serverfunktionen und zur Planung einer verteilten Bereitstellung von Exchange Server 2007 finden Sie im Abschnitt zur Planung und Architektur in Microsoft Exchange Server 2007 unter http://go.microsoft.com/fwlink/?LinkID=87058&clcid=0x409 (möglicherweise in englischer Sprache).

Bewährte Methode: Konfigurieren der Firewall für eine optimale Direct Push-Leistung

Um die Bandbreite des mobilen Clients optimieren zu können, müssen Sie die Folgen der HTTP-Timeouteinstellungen auf die Firewall und andere Geräte kennen, die mit dem Microsoft Exchange-Clientzugriffsserver in Verbindung stehen.

Wenn ein Gerät, für das Direct Push aktiviert ist, eine dauerhafte HTTPS-Verbindung mit Exchange ActiveSync herstellt, gibt es nur zwei Möglichkeiten, mit denen die Verbindung über eine Antwort an den Client zurückgegeben wird. Die erste Möglichkeit besteht, wenn das Postfach des Benutzers geändert wird. Exchange ActiveSync gibt dann eine Antwort an das mobile Gerät zurück, um es zur Synchronisierung mit dem Exchange-Server zu veranlassen. Die zweite Möglichkeit ist gegeben, wenn das Taktintervall der Direct Push-Verbindung abläuft. In diesem Fall weist Exchange ActiveSync das mobile Gerät an, eine neue Direct Push-Anforderung zu senden. Wenn der HTTP-Timeout der Firewall kürzer als das Direct Push-Taktintervall ist, muss das Gerät eine neue Anforderung senden. Im Lauf der Zeit kann das die Bandbreitenauslastung erhöhen. Es wird deshalb empfohlen, den Timeout der Firewall auf 30 Minuten festzulegen. Bei einer längeren Timeoutdauer treten weniger Timeouts auf, was die Bandbreitennutzung verbessert.

Die folgende Abbildung zeigt die empfohlenen Firewalleinstellungen.



Technische Erläuterungen zur Direct Push-Technologie finden Sie unter Grundlegendes zu Direct Push in diesem Dokument.

Sicherheitsfeatures: Authentifizierung und Zertifizierung

Die Verwendung von SSL zum Verschlüsseln des Kanals zwischen dem mobilen Gerät und Exchange ActiveSync wird dringend empfohlen. Dieser Bereitstellungsschritt ist unabhängig von der Größe der Organisation relevant. Einige SSL-Anbieter, die preiswerte SSL-Zertifikate anbieten, haben ihr vertrauenswürdiges Stammzertifikat bereits auf den Windows Mobile-basierten Geräten installiert. Deshalb müssen Sie sich nicht mit jedem einzelnen Gerät beschäftigen.

Eine weitere bewährte Methode besteht darin, den gesamten Internetverkehr über einen Reverseproxy oder eine Firewall, wie z. B. ISA 2006, zu leiten.

Bewährte Methode: Verwenden von SSL zur Verschlüsselung und Serverauthentifizierung

Verschlüsseln Sie zum Schutz der ein- und ausgehenden Daten den gesamten Datenverkehr mit SSL. Sie können SSL-Sicherheitsfeatures auf einem Exchange-Server konfigurieren, um Internetangriffe, wie z. B. Man-in-the-Middle-Angriffe und bestimmte Spoofingangriffe auf Server, besser zu verhindern. Der Exchange-Server erfordert wie jeder Webserver ein gültiges Zertifikat, um SSL-Verbindungen herstellen zu können.
Windows Mobile 6-basierte Geräte sind mit vertrauenswürdigen Stammzertifikaten ausgestattet. Wenden Sie sich an den Gerätehersteller, um eine Liste der Zertifizierungsstellen zu erhalten, die in den Geräten enthalten sind. Wenn Sie ein Stammzertifikat von einem vertrauenswürdigen Anbieter erhalten haben, können die Geräte in der Regel ohne weitere Konfiguration SSL-Verbindungen herstellen. Falls Sie eigene Zertifikate erstellen, müssen Sie diese Zertifikate dem Stammspeicher jedes mobilen Geräts hinzufügen.

Hinweis:

Einige Serverzertifikate werden mit Zwischenstellen in der Zertifizierungskette ausgestellt. Wenn IIS nicht so konfiguriert ist, dass alle Zertifikate der Kette während des SSL-Handshakes an das mobile Gerät gesendet werden, wird das Zertifikat nicht als vertrauenswürdig behandelt. Das liegt daran, dass das Gerät kein dynamisches Abrufen der anderen Zertifikate unterstützt.

Weitere Informationen zu Windows Mobile 6 und Zertifikaten finden Sie unter Schritt 6: Zertifikatregistrierung und Geräteprovisioning.

Bewährte Methode: Festlegen und Bereitstellen einer Kennwortrichtlinie für Geräte

Exchange Server 2007 bietet neue Sicherheitseinstellungen, z. B. Kennwortablauf und Kennwortverlauf, die auf Windows Mobile 6-basierte Geräte angewendet werden können. Ein IT-Experte kann diese Einstellungen mit der Exchange-Verwaltungskonsole verwalten. Weitere Informationen zum Festlegen von Sicherheitsrichtlinien finden Sie in Schritt 5: Konfigurieren und Verwalten des Zugriffs über mobile Geräte auf den Exchange-Server.

Bewährte Methode: Verwenden der Webveröffentlichung mit der Standardauthentifizierung

Viele Unternehmen benötigen eine Standardauthentifizierung über einen verschlüsselten Kanal (SSL). Diese Unternehmen können ihre mobile Bereitstellung noch sicherer gestalten, indem sie ISA 2006 zur Webveröffentlichung auf dem Server mit Exchange Server 2007 nutzen. Der Vorteil der Webveröffentlichungsfunktionen von ISA Server liegt in der integrierten Logik von ISA Server. Diese Logik kann gültige Anforderungen erkennen, z. B. Exchange ActiveSync-Anforderungen, und zum Schutz des Exchange-Clientzugriffsservers vor Angriffen beitragen.

Als bewährte Methode gilt: Die Webveröffentlichung lässt sich leichter implementieren und bietet eine höhere Sicherheit als die Serververöffentlichung.

Szenarien der Netzwerkarchitektur

Dieser Abschnitt enthält Informationen zur Netzwerktopologie für die Bereitstellung von Exchange Server 2007 und Windows Mobile 6. Die folgenden Szenarien werden vorgestellt:

- ISA Server 2006 als erweiterte Firewall (hinter der Firewall eines Drittanbieters)
- Die Verwendung einer Firewall eines Drittanbieters
- Parallele Bereitstellung von Exchange Server 2003 und Exchange Server 2007

Bereitstellungsoptionen

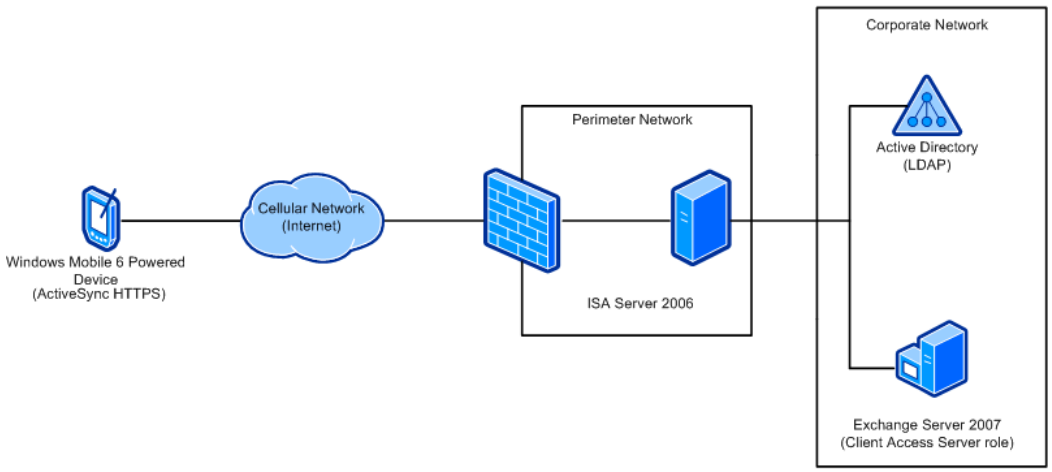
Die folgenden Szenarien sind nur einige der vielen Möglichkeiten zur Implementierung einer Mobile Messaging-Lösung mit Exchange Server 2007, ISA Server 2006, Drittanbieterfirewalls und Windows Mobile 6-basierten Geräten. Die Szenarien werden in neutraler Reihenfolge vorgestellt.

Wichtig:

Diese Optionen veranschaulichen mögliche Bereitstellungsstrategien für das Netzwerk. Bei der letztendlich gewählten Topologie müssen die speziellen Gegebenheiten des Netzwerks berücksichtigt werden. Dazu gehören die verfügbare Hardware und Software, Sicherheitsaspekte, der voraussichtliche Verwendungszweck und die Fähigkeit, für eine optimale Leistung zu sorgen. Gehen Sie vor der Implementierung alle Sicherheitsaspekte des Netzwerks gründlich durch. Hinweise zu Referenzmaterial für ISA Server finden Sie unter Schritt 4: Installieren und Konfigurieren von ISA Server 2006 oder einer anderen Firewall. Informieren Sie sich bei Firewalls von Drittanbietern in der Dokumentation des Herstellers über die entsprechenden Sicherheitsthemen.

Option 1: ISA Server 2006 als erweiterte Firewall in einem Perimeternetzwerk

Als erste Option wird die Implementierung von ISA Server 2006 als Sicherheitsgateway vorgestellt. ISA Server 2006 und Exchange Server 2007 erweitern die Sicherheitsfeatures, indem zusätzlich zu SSL-Bridging und Benutzerauthentifizierung eine Protokollüberprüfung bereitgestellt wird.



Hinweis:

Der Computer mit ISA Server fungiert als erweiterte Firewall im Perimeternetzwerk, das den Internetdatenverkehr aufnimmt. Er kommuniziert direkt mit den LDAP-Servern und den internen Exchange-Servern. Der Computer mit ISA Server erhöht die Sicherheit, da er alle SSL-Clientanforderungen abfängt und an die Exchange-Back-End-Server weiterleitet.

In dieser Konfiguration liegen die Exchange-Server innerhalb des Unternehmensnetzwerks, und der Computer mit ISA Server fungiert als erweiterte Firewall im Perimeternetzwerk. Das ergibt eine zusätzliche Sicherheitsschicht für das Netzwerk.

Der gesamte über Port 443 eingehende Datenverkehr aus dem Internet wird von ISA Server 2006 abgefangen. ISA Server beendet die SSL-Verbindung, authentifiziert den Benutzer und überprüft die Anforderung. Gültige Anforderungen werden dann zur Verarbeitung an den Exchange-Clientzugriffsserver weitergeleitet.

Weitere Informationen zum Exchange-Clientzugriff finden Sie unter Konfigurieren von ISA Server 2006 für Exchange-Clientzugriff (möglicherweise in englischer Sprache).

Die folgende Tabelle enthält Überlegungen zur Bereitstellung von ISA Server 2006 als erweiterte Firewall in einem Perimeternetzwerk, als Domänenmitglied und weitere mögliche ISA-Topologien.

Einrichtungs-typ	Beschreibung	Weitere Überlegungen
Firewall in Arbeitsgruppe, in Perimeter-netzwerk	• Alle Exchange-Server befinden sich im Unternehmensnetzwerk. • FBA- oder Standardauthentifizierung • SSL ist für Exchange ActiveSync zur Verschlüsselung des gesamten Messagingverkehrs konfiguriert. • ISA Server fungiert als erweiterte Firewall im Perimeternetzwerk, das den Internetdatenverkehr aufnimmt. • ISA Server 2006 kommuniziert direkt mit LDAP- und RADIUS-Servern. • LDAP-Authentifizierung • LDAP, LDAPS, LDAP-GC und LDAPS-GC werden unterstützt. • Da jeder Domänencontroller nur die Benutzer seiner Domäne authentifizieren kann, fragt ISA Server standardmäßig den globalen Katalog für eine Gesamtstruktur ab, um die Anmeldeinformationen des Benutzers zu überprüfen. • RADIUS-Authentifizierung	• Der gesamte Exchange-Datenverkehr wird im Voraus authentifiziert, was Angriffsfläche und Risiko reduziert. • Die Clientauthentifizierung für Exchange ist mit Windows, Kerberos, LDAP, LDAPS, RADIUS oder RSA SecurID möglich. Die Clientauthentifizierung für ISA Server ist auf FBA, Standard, LDAP und RADIUS beschränkt. • Port 443 muss in der Firewall für eingehenden und ausgehenden Internet-Datenverkehr geöffnet sein. • Ein digitales Zertifikat zum Herstellen einer Verbindung mit dem Konfigurationsspeicherserver ist erforderlich. • Auf Konfigurationsspeicherserver beschränkt (ADAM-Einschränkung). • Domänenadministratoren haben keinen Zugriff auf das Firewallarray. • Arbeitsgruppenclients können die Windows-Authentifizierung nicht verwenden. • Gespiegelte Konten zum Überwachen von Arrays müssen verwaltet werden. Weitere Informationen zur ISA-Authentifizierung finden Sie unter http://go.microsoft.com/fwlink/?LinkID=87060&clcid=0x409 (möglicherweise in englischer Sprache.)

	• RADIUS stellt die Überprüfung der Anmeldeinformationen bereit. • ISA Server ist je nach RADIUS-Authentifizierungsantwort der RADIUS-Client. Kennwortänderungen sind nicht möglich.	
ISA Server 2006 in einer Domäne, im Perimeter-netzwerk	• Exchange-Clientzugriffsserver (CAS in der Unternehmens-gesamtstruktur) • Als Domänenmitglied kommuniziert ISA Server 2006 mit Active Directory.	• Um die Kommunikation der Domänenmitglieder mit Active Directory zu vereinfachen, werden zusätzliche Ports in der internen Firewall geöffnet. • IPSec kann zwischen dem Computer mit ISA Server und dem Exchange-Server konfiguriert werden, sodass keine weiteren offenen Ports mehr erforderlich sind. • Einige Organisationen möchten möglicherweise Domänenressourcen außerhalb des vertrauenswürdigen LANs vermeiden. Das könnte bei einigen Topologien ein Sicherheitsrisiko darstellen.
ISA Server 2006 in einer Domäne, in der Unternehmens-gesamtstruktur	• Exchange-Front-End in der Unternehmensgesamtstruktur • Als Unternehmens-domänenmitglied fungiert ISA als vertrauenswürdiges Domänenmitglied, das auch den Domänenrichtlinien folgt. Ermöglicht außerdem eine sicherere CSS-Bereitstellung.	• Keine speziellen Firewallports oder IPSec-Tunnels sind erforderlich; KCD funktioniert reibungsloser.

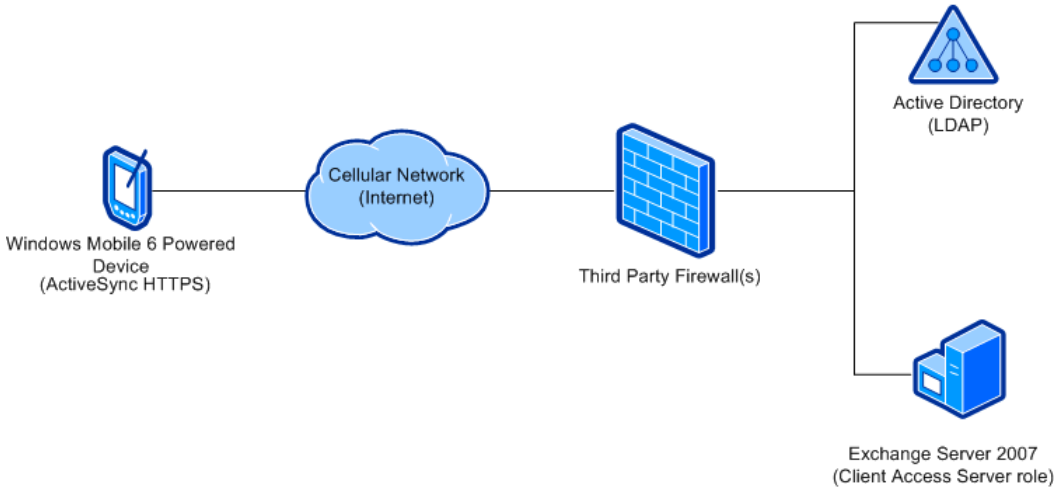
Option 2: Firewall eines Drittanbieters

Als zweite Option wird die Bereitstellung der Mobile Messaging-Lösung mit der Firewall eines Drittanbieters vorgestellt. Die folgenden Bedingungen sollten erfüllt sein, damit eine effiziente und sichere Architektur erstellt werden kann:

- Verwenden Sie SSL zum Verschlüsseln des Datenverkehrs zwischen dem mobilen Gerät und Exchange Server 2007.
- Öffnen Sie den eingehenden Port 443 in jeder Firewall zwischen dem mobilen Gerät und Exchange Server.
- Legen Sie das Zeitlimit für Leerlaufsitzungen für alle Firewalls und Netzwerkgeräte im Pfad zwischen dem mobilen Gerät und Exchange Server auf 30 Minuten fest, um die Bandbreite für die Direct Push-Technologie zu optimieren.

Hinweis:

Anweisungen zum Öffnen des eingehenden Ports 443 und zur Einstellung des Zeitlimits für Leerlaufsitzungen finden Sie in der Dokumentation des Herstellers der Firewall. Weitere Informationen und Richtlinien zu Direct Push finden Sie unter Grundlegendes zu Direct Push.



Einrichtungstyp	Beschreibung	Weitere Überlegungen
Firewall eines Drittanbieters	Öffnen Sie in der Firewall des Drittanbieters den eingehenden Port 443. Konfigurieren Sie den Direct Push-Zugriff für mobile Geräte.	Zur Bereitstellung von Mobile Messaging ist keine zusätzliche Hardware oder Software erforderlich.

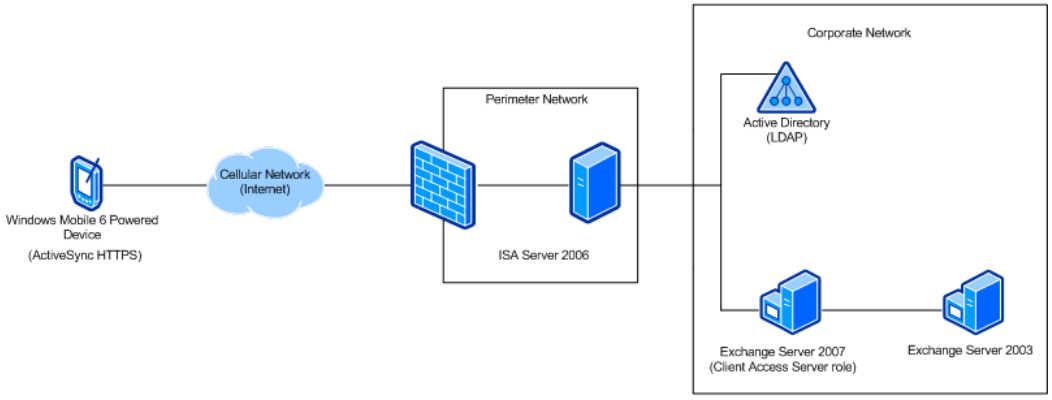
Option 3: Parallele Bereitstellung von Exchange Server 2007 und Exchange Server 2003

Wenn eine Organisation ihre Unternehmensarchitektur nicht auf Exchange Server 2007 umstellen möchte, gibt es noch eine dritte Alternative. Bei einer Front-End-Serverinstallation können einige neue Features des Exchange Server 2007-Clientzugriffsservers für mobile Clients verwendet werden.

Hinweis:

Die folgende Abbildung zeigt zwar eine mögliche IT-Infrastruktur, es wird jedoch dringend empfohlen, für alle Server eines Standorts die gleiche Version von Microsoft Exchange zu verwenden.

Bereitstellen von Windows Mobile 6-basierten Geräten mit Microsoft Exchange Server 2007



Welche Version von Exchange ActiveSync von Clients verwendet wird, hängt auch von der Version des Servers ab, auf dem sich das Postfach des Benutzers befindet. Wenn ein Client eine Verbindung mit dem Exchange Server 2007-Clientzugriffsserver herstellt, wird vom System geprüft, wo sich die Benutzerdaten befinden. Wenn sie auf einem 2003-Postfachserver gespeichert sind, wird die Version Exchange Server 2003 des ActiveSync-Protokolls verwendet. Befindet sich das Postfach des Benutzers auf einem Exchange Server 2007-Postfachserver, wird die Verbindung an den Postfachserver weitergeleitet, auf dem die neue Version von ActiveSync mit dem Gerät verwendet wird. Ein Benutzer, dessen Postfach in einer früheren Serverversion gespeichert ist, kann deshalb die neuen Features nicht verwenden, wie z. B. Zugriff auf SharePoint-/UNC-Dokumente und Exchange-Suche. Denn das ActiveSync-Protokoll unterstützt diese Anforderungen nicht.

Hinweis:

Damit die Exchange-Suche sowie andere Features und Richtlinien funktionieren, müssen sie vom Gerät unterstützt werden. Derzeit werden Richtlinien und Features, die in Exchange 2003 SP2 nicht vorhanden waren, von Windows Mobile 5 nicht unterstützt.

Die Verwendung des Exchange-Clientzugriffsservers im Perimeternetzwerk bietet folgende zusätzliche Vorteile:

- Neue Exchange-Verwaltungsfunktionen.
- Neue Exchange-Verwaltungsfunktionen für mobile Geräte.
- Erweiterte Exchange-Protokollierung (Export nach SQL Server und Excel).
- Möglichkeit, nur die Verbindung von Geräten zuzulassen, die mit Provisioning konfiguriert sind.

Wichtig:

Die folgenden Features können in der Paralleltopologie nicht verwendet werden, sondern erfordern einen Exchange Server 2007-Clientzugriffsserver und einen Exchange Server 2007-Postfachserver:

- Remoteeinstellung von Abwesenheitsantworten
- Zugriff auf SharePoint- und UNC-Dokumente
- Kennzeichnung von E-Mail
- Durchsuchen des Postfachs nach E-Mail
- Erweitertes Anzeigen von Teilnehmern
- Neue Features zu Sicherheitsrichtlinien für die Smartcardverschlüsselung

- Gruppenbasierte Richtlinien
- Alle sonstigen Features, die sich auf die neue Version von ActiveSync oder des Benutzerpostfachs beziehen.

Bei der Umstellung von Exchange Server 2003 auf Exchange Server 2007 migrieren Sie in der Regel alle Exchange-Server in einer bestimmten Routinggruppe oder einem Active Directory-Standort gleichzeitig, konfigurieren die Parallelinstallation und migrieren dann den nächsten Standort.

Wichtig:

Stellen Sie fest, ob Sie Einstellungen für Outlook Web Access oder benutzerdefinierte Konfigurationen, Sicherheitsupdates, Designs und Anpassungskonfigurationen der Exchange Server 2003-Front-End-Server beibehalten möchten, bevor Sie die Clientzugriffsserver konfigurieren und die Exchange 2003-Front-End-Server außer Betrieb nehmen. Für die Installation von Exchange Server 2007 ist eine 64-Bit-Hardware erforderlich. Bei der Installation werden keine Einstellungen oder benutzerdefinierten Konfigurationen aus Exchange Server 2003 übernommen. Stellen Sie deshalb sicher, dass die Einstellungen für Outlook Web Access und benutzerdefinierten Konfigurationen auf dem Exchange Server 2003-Back-End-Server mit den Konfigurationen auf dem Exchange Server 2003-Front-End-Server übereinstimmen. Anschließend können Sie die Front-End-Server außer Betrieb nehmen und den Clientzugriffsserver installieren.

Wenn Sie die Serverfunktionen auf verschiedener Hardware installieren, sollten Sie die Serverfunktionen in der folgenden Reihenfolge bereitstellen:

1. Installieren Sie zuerst die Client Access-Serverfunktion, um alle Front-End-Server zu ersetzen.
2. Stellen Sie die Hub-Transport-Serverfunktion bereit, und konfigurieren Sie die Routinggruppenconnectors, Sendeconnectors und Empfangsconnectors.
3. Stellen Sie die Mailbox-Serverfunktion bereit, und verschieben Sie die Postfächer auf den neuen Server.

Hinweis:

Weitere Informationen zur Installation von Exchange Server 2007 in der Organisation finden Sie unter Schritt 1: Installieren von Exchange Server 2007 mit der Client Access-Serverfunktion.

Einrichtungstyp	Beschreibung	Weitere Überlegungen
Exchange Server 2007-Clientzugriffsserver und Exchange Server 2003-Netzwerk im Unternehmensnetzwerk.	Exchange 2007/2003 werden im Front-End- und Back-End-Stil verwendet. Möglichkeit zur Verwendung der Exchange Server 2007-Verwaltungsfunktionen.	Alle Server an einem Standort sollten dieselbe Exchange-Version verwenden.

Authentifizierung in ISA Server 2006

Benutzer können mit der integrierten Windows-, LDAP-, RADIUS- oder RSA SecurID-Authentifizierung authentifiziert werden. Front-End- und Back-End-Konfigurationen sind getrennt worden, was eine größere Flexibilität und detailliertere Steuerung ermöglicht. Für die Authentifizierung auf Websites wird das einmalige Anmelden unterstützt. In jedem Namespace können für Benutzer oder Benutzergruppen Regeln angewendet werden.

Für die meisten Unternehmensinstallationen wird ISA Server 2006 mit LDAP-Authentifizierung empfohlen. Außerdem ermöglicht ISA Server 2006 eine auf Zertifikaten basierende Authentifizierung bei der Webveröffentlichung. Weitere Informationen finden Sie unter Authentifizierung in ISA Server 2006 auf der Microsoft TechNet-Website (möglicherweise in englischer Sprache).

Die folgende Tabelle enthält eine Übersicht einiger Features von ISA Server 2006:

Feature	Beschreibung
Unterstützung der LDAP-Authentifizierung	Mithilfe der LDAP-Authentifizierung kann der Computer mit ISA Server die Authentifizierung für Active Directory ausführen, ohne ein Mitglied der Domäne zu sein. Weitere Informationen finden Sie unter http://go.microsoft.com/fwlink/?LinkID=87069&clcid=0x409 (möglicherweise in englischer Sprache).
Authentifizierungsdelegierung	Veröffentlichte Websites sind vor nicht authentifiziertem Zugriff geschützt, da die ISA Server 2006-Firewall den Benutzer authentifiziert, bevor die Verbindung an die veröffentlichte Website weitergeleitet wird. So können Angriffe nicht authentifizierter Benutzer den veröffentlichten Webserver nicht erreichen. Diese Funktionalität wird unter Authentifizierung in ISA Server 2006 (möglicherweise in englischer Sprache) näher erläutert.
SecurID-Authentifizierung für Webproxyclients	ISA Server 2006 kann Remoteverbindungen über die zweistufige SecurID-Authentifizierung authentifizieren. So wird bei der Authentifizierung ein hohes Maß an Sicherheit erzielt, da ein Benutzer über verschiedene Informationen verfügen muss, um Zugriff auf den veröffentlichten Webserver zu erhalten.
RADIUS-Unterstützung für Webproxyclient-Authentifizierung	Mit ISA Server 2006 können Sie Benutzer in Active Directory und anderen Authentifizierungs-datenbanken authentifizieren, indem Sie für die Active Directory-Abfragen RADIUS verwenden. Webveröffentlichungsregeln können für die Authentifizierung von Remotezugriffsverbindungen ebenfalls RADIUS verwenden.

Formularbasierte Authentifizierung mit Kennwort und Passphrase	ISA Server 2006 ermöglicht eine zweistufige Authentifizierung. Dabei verwenden Sie Benutzernamen/Kennwort in Verbindung mit einer Passphrase (SecureID/RADIUS OTP).
Sitzungsverwaltung	ISA Server 2006 bietet ein bessere Steuerung cookiebasierter Sitzungen und verbessert dadurch die Sicherheit und SSO für webbasierte Clients wie OWA.
Zertifikatverwaltung	ISA Server 2006 vereinfacht die Zertifikatverwaltung. Pro Weblistener können mehrere Zertifikate genutzt und pro Arraymitglied können verschiedene Zertifikate verwendet werden.

Weitere Informationen zum Konfigurieren von ISA Server 2006 für Exchange 2007 finden Sie unter Konfigurieren von ISA Server 2006 für Exchange-Clientzugriff (möglicherweise in englischer Sprache).

Grundlegendes zu Direct Push

Bei der Direct Push-Technologie wird Exchange ActiveSync verwendet, um Daten auf einem Windows Mobile-basierten Gerät mit Daten auf einem Microsoft Exchange-Server zu synchronisieren. SMS ist für die Benachrichtigung nicht mehr erforderlich.

Direct Push-Technologie

Die Direct Push-Technologie besteht aus zwei Teilen: ein Teil befindet sich auf dem Gerät (Client) und der andere Teil auf einem Exchange Server 2007-Mailserver. In der folgenden Liste werden diese beiden Teile der Technologie beschrieben:

- Windows Mobile 6-basierte Geräte. Mit der ActiveSync-Technologie auf dem Gerät wird die Direct Push-Kommunikation mit dem Exchange-Server verwaltet. ActiveSync stellt für einen angegebenen Zeitraum eine HTTP- oder HTTPS-Verbindung mit dem Server her und wechselt dann in den Ruhezustand, bis der Server antwortet. Der Server antwortet mit einer Statusmeldung, die angibt, ob neue Elemente empfangen oder nicht empfangen wurden. Anschließend sendet das Gerät eine Synchronisierungsanforderung oder eine weitere Direct Push-Anforderung. Das Intervall, nach dem dieser Vorgang stattfindet, wird dynamisch angepasst. Diese Anpassung basiert auf Parametern, die vom OEM oder Mobilfunkbetreiber festgelegt wurden, und darauf, wie lange eine HTTP- oder HTTPS-Verbindung im Leerlauf im Netzwerk des Betreibers und dem Unternehmensnetzwerk des Kunden bestehen bleiben kann.
- Exchange Server 2007 (Client Access-Serverfunktion ist installiert). Diese Version von Exchange Server enthält eine Direct Push-Komponente, die die Exchange ActiveSync-Infrastruktur durch die Möglichkeit manueller und geplanter Synchronisierungen ergänzt. Exchange Server sendet E-Mail-Nachrichten, Kalenderdaten und Aufgabenaktualisierungen anhand von IP-Benachrichtigungen an ein Gerät, sobald diese Informationen auf dem Server eintreffen.

Datenänderungen auf dem Server werden über eine dauerhafte HTTP- oder HTTPS-Verbindung, die für Direct Push verwendet wird, sofort an das Gerät übertragen. Der Timeoutwert im Netzwerk des Mobilfunkbetreibers gibt an, wie lange die dauerhafte Verbindung bei ausbleibender Aktivität bestehen bleibt.

Um den Timeout zwischen den Aktualisierungen zu verhindern, sendet das Gerät eine neue Anforderung, sobald der Server reagiert. Diese regelmäßige Übertragung wird Takt genannt. Der Takt hält die Verbindung mit dem Server für Direct Push aufrecht. Dabei signalisiert jeder Takt dem Server, dass das Gerät empfangsbereit ist.

Der Direct Push-Vorgang

Der Direct Push-Verkehr ähnelt kleinen HTTP-Anfragen an eine Internetwebsite, die viel Zeit für eine Antwort beansprucht. Verschlüsseln Sie möglichst den Inhalt der Pakete mit Secure Sockets Layer (SSL), um den Direct Push-Verkehr vor Sniffing zu schützen.

Die folgenden Schritte erläutern den Direct Push-Vorgang:

1. Der Client sendet eine HTTP-Nachricht, eine so genannte Ping-Anforderung, an einen Exchange-Server. Damit wird der Server zur Übermittlung eventueller Änderungen aufgefordert, die im Postfach des Benutzers innerhalb einer angegebenen Zeitspanne aufgetreten sind. In der Ping-Anforderung gibt der Client die Ordner an, deren Änderung von Exchange überwacht werden soll. In der Regel handelt es sich hierbei um Posteingang, Kalender, Kontakte und Aufgaben.

2. Wenn Exchange diese Anforderung empfängt, werden die angegebenen Ordner überwacht, bis Folgendes eintritt:
   - Das Zeitlimit läuft ab. Das Zeitlimit wird durch den kürzesten Timeout im Netzwerkpfad bestimmt. In diesem Fall sendet Exchange eine „HTTP 200 OK“-Antwort an den Client.
   - Der Ordnerinhalt ändert sich, z. B. durch den Eingang einer E-Mail-Nachricht. In diesem Fall sendet Exchange eine Antwort auf die Anforderung und identifiziert den Ordner, in dem die Änderung stattfand.
3. Der Client reagiert folgendermaßen auf die Antwort des Exchange-Servers:
   - Wenn er eine „HTTP 200 OK“-Antwort empfängt, d. h. keine Änderung erfolgt ist, sendet er eine erneute Ping-Anforderung.
   - Wenn er eine andere Antwort als „HTTP 200 OK“ empfängt, sendet er eine Synchronisierungsanforderung an jeden geänderten Ordner. Nach Abschluss der Synchronisierung sendet der Client erneut die Ping-Anforderung.
   - Empfängt der Client innerhalb der angegebenen Zeitspanne keine Antwort vom Exchange-Server, verkürzt er das Zeitintervall in der Ping-Anforderung und sendet die Anforderung erneut.

Direct Push-Anpassung

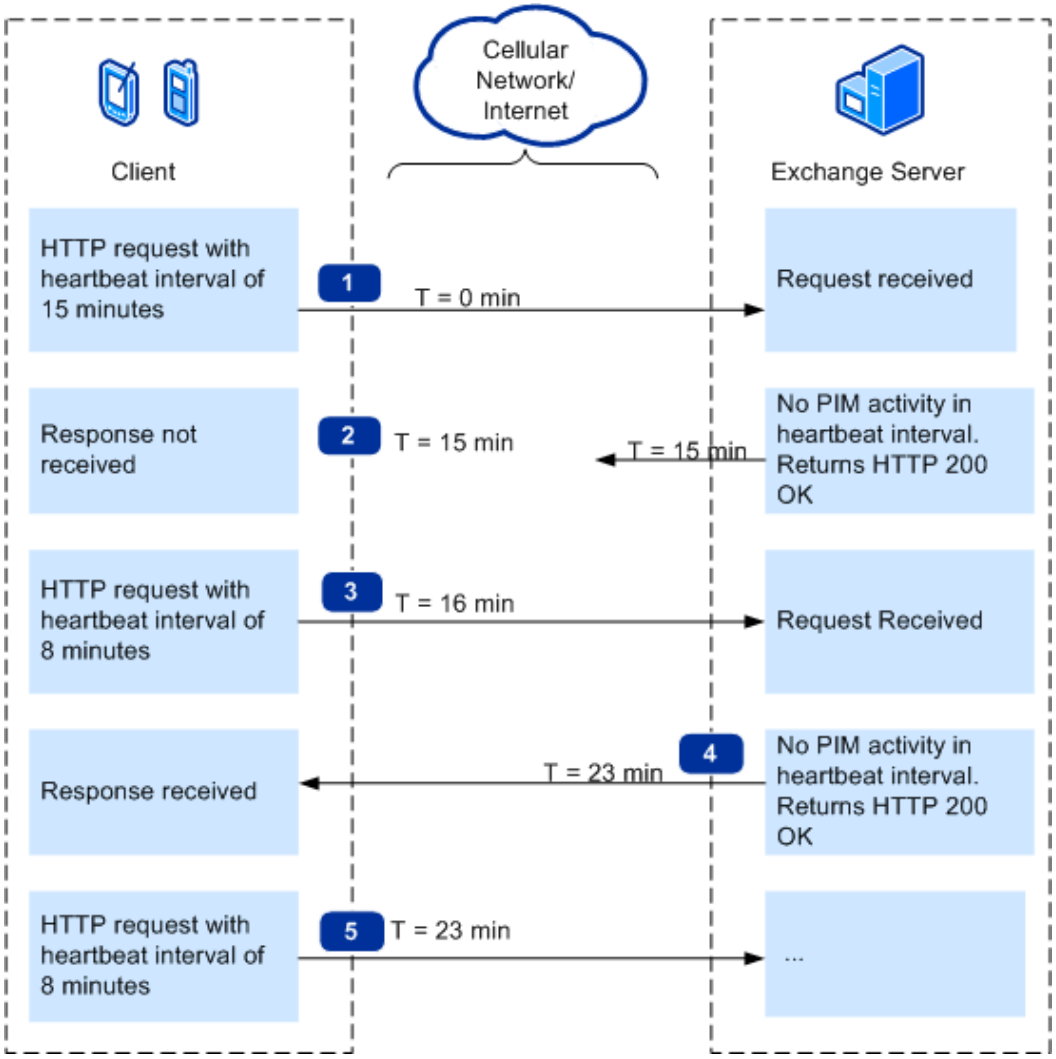
Während des Direct Push-Vorgangs wartet das Gerät aufeinanderfolgende Roundtrips ab. Erst dann passt es die Zeitspanne an, in der eine Verbindung mit dem Server aufrechterhalten bleiben muss. Die Zeitspanne, die der Server auf PIM-Änderungen oder auf den Eingang neuer E-Mail-Nachrichten wartet, bevor die OK-Antwort an den Client gesendet wird, ist das Taktintervall.

Das Taktintervall wird vom Client angegeben und im Rahmen der Ping-Anforderung übermittelt. Der Takt beginnt mit der Standarddauer. Der Direct Push-Algorithmus auf dem Client passt dann das Taktintervall dynamisch an, um die maximale Zeitspanne zwischen den Takten ohne Überschreitung des Timeoutwerts zu erhalten. Die Anpassung hängt von den Netzwerkbedingungen ab und davon, wie lange eine HTTP- oder HTTPS-Verbindung im Netzwerk des Mobilfunkbetreibers oder dem Unternehmensnetzwerk erhalten bleiben kann. Außerdem kann der Mobilfunkbetreiber bestimmte Einstellungen entsprechend festgelegt haben.

Der Algorithmus führt ein Protokoll der Ping-Anforderung zur Ermittlung des optimalen Taktintervalls. Folgt eine Antwort auf die Ping-Anforderung, erhöht der Algorithmus das Intervall. Ist am Ende des Intervalls keine Antwort eingegangen, geht der Client von einem Netzwerktimeout aus und verringert das Intervall.

Anhand des Algorithmus ermittelt der Client die längste Zeitspanne, die sich eine Verbindung in einem Funknetzwerk und der Unternehmensfirewall im Leerlauf befinden kann.

Die folgende Abbildung zeigt, wie das Taktintervall bei einer typischen Direct Push-Kommunikation zwischen dem Client und dem Exchange-Server angepasst wird.



„T“ in der Abbildung zeigt den Verlauf des Taktintervalls.

Die Kommunikation wird in den folgenden Schritten beschrieben. Die Zahlen entsprechen den Zahlen in der Abbildung:

1. Der Client wird aktiv und sendet über das Internet eine HTTP-Anforderung an den Exchange-Server. Anschließend wechselt er in den Ruhezustand.

   Damit die Sitzung aktiv bleibt, gibt die Anforderung das Taktintervall an. Das ist die Zeitspanne, die der Server auf PIM-Änderungen oder auf den Eingang neuer E-Mail-Nachrichten warten soll, bevor er die OK-Antwort an den Client sendet. In der Abbildung beträgt das Taktintervall 15 Minuten.

2. Da während des Taktintervalls keine E-Mail-Nachricht eingegangen ist, gibt der Server eine „HTTP 200 OK“-Antwort zurück.

   In diesem Beispiel ist die Antwort verloren gegangen, weil das Betreibernetzwerk oder das Unternehmensnetzwerk die dauerhafte HTTP-Verbindung nicht aufrechterhalten konnte. Der Client erhält die Antwort somit nicht.

3. Der Client wird am Ende des Taktintervalls plus 1 Minute (15 + 1 = 16 Minuten insgesamt) aktiv.

- **Hinweis:** Das Gerät wartet wiederholte Roundtrips ab, bevor es das Taktintervall anpasst. Mit einer Abstimmungskomponente im Algorithmus kann die angegebene Zeitabstufung geändert werden.

Wenn ein wiederholter Roundtrip ohne Antwort vom Server folgt, sendet der Client eine kürzere Anforderung (8 Minuten).

In diesem Beispiel wird der Takt auf einen Mindesttaktwert (8 Minuten) geändert, da der Takt während des letzten Pings nicht erhöht worden ist.

4. Da während des Taktintervalls keine E-Mail-Nachricht eingegangen ist, gibt der Server eine „HTTP 200 OK“-Antwort zurück.
5. Durch die Serverantwort wird der Client aktiv. Nachdem während des Intervalls kein Timeout erfolgt ist, erkennt der Client, dass das Netzwerk Leerlaufverbindungen von mindestens dieser Dauer unterstützt.

   Wenn es sich um einen wiederholten Roundtrip handelt, kann der Client das Intervall für die nächste Anforderung erhöhen.

Auswirkungen von Direct Push auf Netzwerke und Exchange-Server

Der Algorithmus, der den Takt festlegt, minimiert außerdem die über ein Funknetzwerk übertragenen Bytes und schont die Lebensdauer der Batterie.

Die Implementierung einer Datenkomprimierung verringert die Größe der zwischen dem Exchange-Server (Client Access-Serverfunktion) und dem Client übermittelten Pakete. Die beanspruchte Bandbreite und die entsprechenden Auswirkungen auf den Datenplan des Benutzers hängt größtenteils von den folgenden Faktoren ab:

- Welche Daten der Benutzer synchronisiert, z. B. mehr als nur die Standardordner.
- Wie viele Daten im Postfach und auf den mobilen Geräten geändert werden.

Auswirkungen von Änderungen der Direct Push-Einstellungen

Für die verschiedenen Direct Push-Einstellungen werden bestimmte Werte empfohlen, damit eine angemessene Leistung während des Direct Push-Vorgangs sichergestellt ist.

Taktintervall

Der Mobilfunkbetreiber legt das Taktintervall im Gerät fest. Ein Taktintervall von 30 Minuten schont die Lebensdauer der Batterie. Wenn die Direct Push-Sitzungen länger dauern (z. B. 30 Minuten), gibt es weniger HTTP-Roundtrips, weniger gesendete und empfangene Daten und einen geringeren Energieverbrauch des Geräts.

Bei einem zu kurzen Taktintervall ist der Benutzer zwar stets auf dem Laufenden, die Batterie wird jedoch wegen der ständigen Ping-Anforderungen an den Server stärker beansprucht.

Mindesttaktintervall

Wenn ein Gerät mit einem niedrigeren Taktintervall als dem Mindesttaktintervall eine Verbindung mit dem Exchange-Server anfordert, warnt der Server den Administrator durch einen Eintrag im Ereignisprotokoll, dass das Direct Push nicht funktioniert.

Exchange-Sitzung

Damit die Geräteinformationen aktuell sind und die Batterie geschont wird, sollte die Dauer der Exchange-Serversitzung etwas höher sein als das Maximaltaktintervall. Wenn die Sitzung kürzer ist, wird möglicherweise

das Zeitlimit für den Leerlauf überschritten, und die Sitzung wird beendet. Die Folge wäre, dass E-Mail-Nachrichten erst übermittelt werden, wenn der Client erneut die Verbindung herstellt. Die Daten des Benutzers werden dann vielleicht längere Zeit nicht synchronisiert.

Firewalltimeouts

Das Zeitlimit für den Leerlauf einer Netzwerkverbindung gibt an, wie lange eine Verbindung nach dem vollständigen Herstellen einer TCP-Verbindung ohne Datenverkehr bestehen bleiben kann.

Das Sitzungsintervall der Firewall muss so festgelegt werden, dass das Taktintervall und das Sitzungsintervall des Unternehmens eine effektive Kommunikation zulassen. Falls die Firewall die Sitzung beendet, würden E-Mail-Nachrichten erst übermittelt werden, wenn der Client erneut die Verbindung herstellt. Die Daten des Benutzers werden dann vielleicht längere Zeit nicht synchronisiert. Wenn die Einstellung für das Sitzungszeitlimit der Firewall gleich oder größer gleich dem Leerlaufzeitlimit des Mobilfunknetzwerks ist, beendet die Firewall die Sitzung nicht.

Legen Sie für die Leerlaufverbindung der Firewall folgende Timeoutwerte fest:

- Mobilfunkbetreiber sollten die Werte für das Zeitlimit für Leerlaufverbindungen bei Firewalls für ausgehende Verbindungen auf 30 Minuten festlegen.
- Bei Firewalls für eingehende Verbindungen benötigen Unternehmen einen Timeoutwert von 30 Minuten.

Webserver, Netzwerksicherheitsgeräte und Netzwerkstapel besitzen verschiedene zeitliche Schwellenwerte als Schutz vor unzureichend getesteten oder böswilligen Clients. Sie können die Einstellung für das Zeitlimit der Leerlaufverbindung problemlos erhöhen, ohne die Sicherheit des Netzwerks zu gefährden.

In einem Direct Push-Szenario ist eine Verbindung zwischen dem Zeitpunkt, zu dem die HTTP-Anforderung gesendet wurde, und folgenden Zeitpunkten im Leerlauf: 1. dem Zeitpunkt, zu dem das Taktintervall abläuft; 2. dem Zeitpunkt, zu dem der Server auf die Anforderung eine Änderung zurückgibt (z. B. beim Empfang von E-Mail). Direct Push setzt keine bestimmte Sitzungsdauer voraus. E-Mail-Nachrichten werden schnell übertragen, unabhängig davon, ob das Taktintervall bei einer Minute oder 30 Minuten liegt.

Eine Erhöhung des Zeitlimits für Leerlaufverbindungen hat keinen Einfluss auf das Angriffsrisiko. Die folgende Tabelle zeigt Beispiele von Angriffen und beschreibt weitere Einstellungen, durch die das Risiko verringert werden kann.

Denial-of-Service-Angriffe (DoS)	Verringerung des Angriffsrisikos
Ein DoS-Angriff erfolgt dadurch, dass die Handshake-Sequenz zum Herstellen einer TCP-Verbindung nicht vollständig abgeschlossen wird. Der Angreifer versucht, eine Vielzahl teilweise geöffneter TCP-Verbindungen zu erstellen.	Eine Erhöhung des Zeitlimits für Leerlaufverbindungen hat keinen Einfluss auf diesen Angriffstyp. Die Zeitspanne, in der ein TCP-Handshake abgeschlossen sein muss, ist ein gesonderter Schwellenwert, der vom TCP/IP-Stapel von Windows bestimmt wird.
Ein DoS-Angriff wird gegen IIS unternommen, indem eine große Anzahl TCP-Verbindungen geöffnet wird, ohne dass eine einzige HTTP-Anforderung erfolgt.	Eine Erhöhung des Zeitlimits für Leerlaufverbindungen hat keinen Einfluss auf diesen Angriffstyp. IIS verringert diese Gefahr dadurch, dass ein Client innerhalb einer bestimmten Zeit eine gültige HTTP-Anforderung senden muss, sonst wird die Verbindung getrennt. Die Einstellungsbezeichnung des Verbindungstimeouts in der IIS-Verwaltungskonsole ist irreführend. TCP-Verbindungen werden beendet, wenn der Wert des Verbindungstimeouts überschritten wird (standardmäßig 120 Sekunden).
Ein Angreifer stellt eine große Anzahl TCP-Verbindungen her und leitet über alle Verbindungen HTTP-Anforderungen, ohne die Antworten entgegenzunehmen.	Eine Erhöhung des Zeitlimits für Leerlaufverbindungen hat keinen Einfluss auf diesen Angriffstyp. Die Gefahr wird mit demselben Timeoutwert verringert wie im vorherigen Szenario. Die Einstellung für den Verbindungstimeout in IIS definiert, innerhalb welcher Zeit ein Client die erste Anforderung nach dem Herstellen der TCP-Verbindung oder eine Folgeanforderung in einem HTTP-Keep-Alive-Szenario senden muss. **Hinweis:** Betrifft nur Exchange ActiveSync-Listener.

Bereitstellungsverfahren zu Windows Mobile 6 und Exchange Server 2007

In dieser Dokumentation werden die Verfahren zur Bereitstellung der Windows Mobile 6-Software und einer Exchange Server 2007-Implementierung beschrieben. Microsoft Internet Security and Acceleration Server 2006 ist für eine Mobile Messaging-Infrastruktur zwar keine Voraussetzung, die Installation wird jedoch empfohlen. Im folgenden Schritt 4 werden die Installationsverfahren für diese Plattform beschrieben.

- Schritt 1: Installieren von Exchange Server 2007 mit der Client Access-Serverfunktion
- Schritt 2: Aktualisieren der Server mit Sicherheitspatches
- Schritt 3: Schützen der Kommunikation zwischen Exchange Server 2007 und Windows Mobile 6-basierten Geräten
- Schritt 4: Installieren und Konfigurieren von ISA Server 2006 oder einer anderen Firewall
- Schritt 5: Konfigurieren und Verwalten des Zugriffs über mobile Geräte auf den Exchange-Server
- Schritt 6: Zertifikatregistrierung und Geräteprovisioning
- Schritt 7: Verwalten und Konfigurieren von Windows Mobile 6-basierten Geräten

Schritt 1: Installieren von Exchange Server 2007 mit der Client Access-Serverfunktion

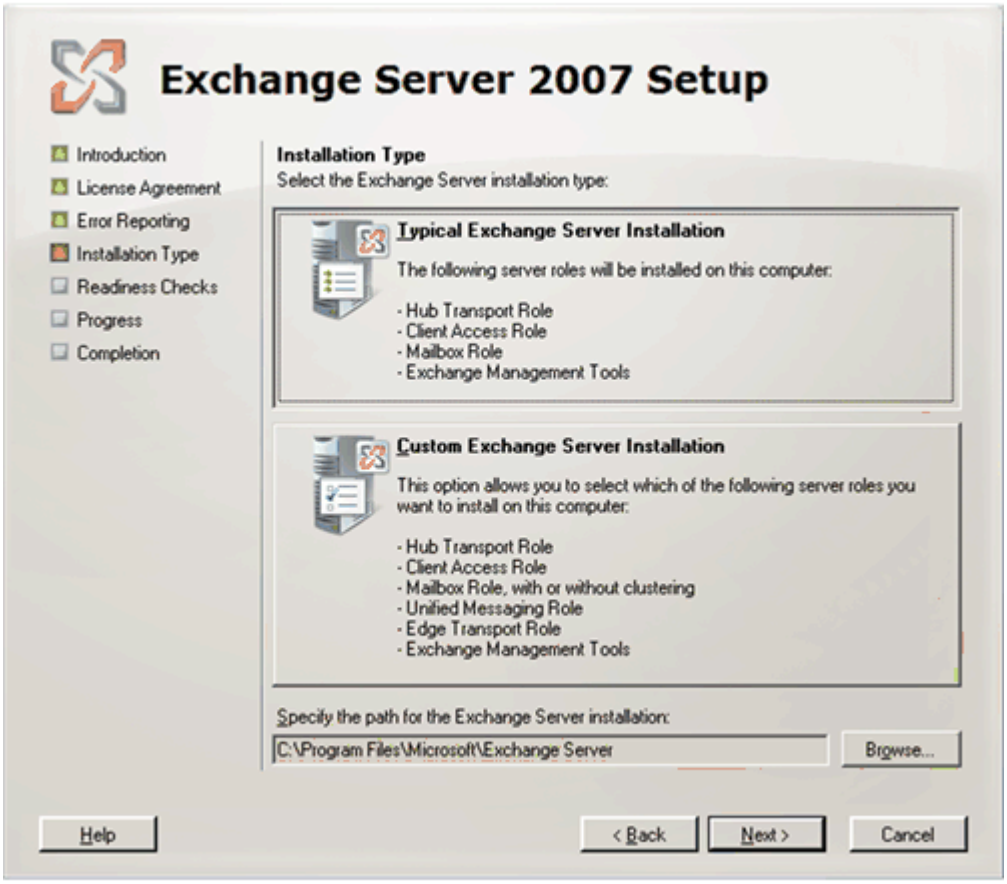
Microsoft Exchange Server 2007 enthält fünf Serverfunktionen, die Sie auf einem Server unter Microsoft Windows Server 2003 installieren können. Die Client Access-Serverfunktion wird für Mobile Messaging-Bereitstellungen benötigt und ermöglicht den Zugriff auf die folgenden Anwendungen und Dienste:

- Microsoft Outlook Web Access
- Exchange ActiveSync
- Post Office Protocol Version 3 (POP3)
- Internet Messaging Application Protocol Version 4 (IMAP4)

Hinweis:
Exchange ActiveSync wird bei Installation der Client Access-Serverfunktion aktiviert.

Die Client Access-Serverfunktion wird standardmäßig bei einer Exchange-Standardinstallation hinzugefügt. Bei einer benutzerdefinierten Exchange-Installation kann sie auch auf einem gesonderten Server installiert werden. Die Entscheidung, ob Exchange Server 2007 auf einem einzelnen Server oder in einer Architektur mit verteilten Funktionen bereitgestellt wird, hängt von den Messagingerfordernissen und Anforderungen der Organisation ab.

Hinweis:
Installieren Sie die Client Access-Serverfunktion nur dann in einem Perimeternetzwerk, wenn Sie Exchange im Rahmen einer Microsoft Small Business Server-Bereitstellung einsetzen. In dieser Konfiguration wird die Verwendung einer Firewall empfohlen, um den an Ihren Clientzugriffsserver geleiteten Internetverkehr zu steuern. Auch das Ausführen eines Exchange Best Practice Analyzer im Vorfeld der Bereitstellung gehört zu den bewährten Methoden. Sie können den Microsoft Exchange Best Practices Analyzer herunterladen: http://go.microsoft.com/fwlink/?LinkID=87079&clcid=0x409.


Exchange Server 2007 Setup
Introduction
License Agreement
Error Reporting
Installation Type
Readiness Checks
Progress
Completion
Installation Type
Select the Exchange Server installation type:
Typical Exchange Server Installation
The following server roles will be installed on this computer:
- Hub Transport Role
- Client Access Role
- Mailbox Role
- Exchange Management Tools
Custom Exchange Server Installation
This option allows you to select which of the following server roles you want to install on this computer:
- Hub Transport Role
- Client Access Role
- Mailbox Role, with or without clustering
- Unified Messaging Role
- Edge Transport Role
- Exchange Management Tools
Specify the path for the Exchange Server installation:
C:\Program Files\Microsoft\Exchange Server
Browse...
Help
< Back
Next >
Cancel

In der folgenden technischen Dokumentation finden Sie Informationen zur Bereitstellung von Microsoft Exchange 2007:

Dokumentation zu Exchange Server 2007
Erste Schritte http://go.microsoft.com/fwlink/?LinkID=91597&clcid=0x409 (möglicherweise in englischer Sprache)
Planung und Architektur http://go.microsoft.com/fwlink/?LinkID=91598&clcid=0x409 (möglicherweise in englischer Sprache)
Microsoft Exchange Server 2007 http://go.microsoft.com/fwlink/?LinkID=91599&clcid=0x409 (möglicherweise in englischer Sprache)
Bereitstellung http://go.microsoft.com/fwlink/?LinkID=91601&clcid=0x409 (möglicherweise in englischer Sprache)
Exchange Server 2007 - Systemanforderungen http://go.microsoft.com/fwlink/?LinkID=91602&clcid=0x409 (möglicherweise in englischer Sprache)

Die Themen in diesen Artikeln behandeln die Planung und Architektur für einfache, standardmäßige, große und komplexe Bereitstellungen von Exchange. Die beschriebenen alternativen Netzwerktopologien unterstützen sowohl eine Standardinstallation (einzelner Server) und eine benutzerdefinierte Installation (mehrere Server).

Bereitstellen von Windows Mobile 6-basierten Geräten mit Microsoft Exchange Server 2007

Hinweis:

In diesem Dokument werden die Verfahren und Richtlinien zur Bereitstellung von Windows Mobile 6 mit Exchange Server 2007 beschrieben. Da nur die Client Access-Serverfunktion und die Mailbox-Serverfunktion bei einem Mobile Messaging-System eine Rolle spielen, werden andere Exchange Server 2007-Serverfunktionen hier nicht erläutert.

Schritt 2: Aktualisieren der Server mit Sicherheitspatches

Bevor Sie beginnen, aktualisieren Sie zuerst die Serverumgebung – alle Exchange-Server, globale Katalogserver und Domänencontroller – mit den neuesten Sicherheitspatches von Microsoft. Dadurch sorgen Sie für ein sicheres Mobile Messaging-End-to-End-Netzwerk.

Besuchen Sie die Microsoft Update-Website, um Ihre Server mit den Sicherheitspatches zu aktualisieren: http://go.microsoft.com/fwlink/?LinkID=87151&clcid=0x409

Weitere Informationen zum Aktualisieren Ihrer Software mit den neuesten Sicherheitspatches finden Sie auf der Website „Exchange Server Security Center“: http://go.microsoft.com/fwlink/?LinkId=62646 (möglicherweise in englischer Sprache).

Weitere Informationen zu Microsoft-Sicherheitsthemen finden Sie auf der Website „Microsoft Security“: http://go.microsoft.com/fwlink/?LinkId=62649 (möglicherweise in englischer Sprache).

Schritt 3: Schützen der Kommunikation zwischen Exchange Server 2007 und Windows Mobile 6-basierten Geräten

Führen Sie diese Schritte aus, um die Kommunikation zwischen dem Exchange-Clientzugriffsserver und Windows Mobile 6-basierten Geräten besser zu schützen:

- Bereitstellen von SSL zum Verschlüsseln des Messagingverkehrs
- Aktivieren von SSL für die Standardwebsite
- Konfigurieren der Standardauthentifizierung für das virtuelle Verzeichnis von Exchange ActiveSync
- Schützen von IIS durch eine Verringerung potenzieller Angriffsflächen

Weitere Informationen zur Authentifizierung und Zertifizierung finden Sie im Abschnitt Bewährte Methoden für die Bereitstellung von Mobile Messaging in diesem Leitfaden.

Bereitstellen von SSL zum Verschlüsseln des Messagingverkehrs

Verschlüsseln Sie zum Schutz der ein- und ausgehenden E-Mail-Nachrichten den Nachrichtenverkehr mit SSL. Sie können SSL-Sicherheitsfeatures auf einem Exchange-Server konfigurieren, um die Integrität von Inhalten und die Identität von Benutzern zu überprüfen und um die Datenübertragungen im Netzwerk zu verschlüsseln. Die folgenden Schritte veranschaulichen, wie SSL für Exchange ActiveSync konfiguriert wird:

1. Anfordern und Installieren eines Serverzertifikats
2. Überprüfen der Installation
3. Sichern des Serverzertifikats
4. Aktivieren von SSL für das virtuelle Verzeichnis von Exchange ActiveSync

Hinweis:

Sie müssen Mitglied der Gruppe **Administratoren** auf dem lokalen Computer sein oder über entsprechende Rechte verfügen, um die folgenden Verfahren ausführen zu können. Es ist eine bewährte Sicherheitsmethode, wenn Sie sich am Computer mit einem Konto anmelden, das nicht zur Gruppe **Administratoren** gehört. Führen Sie dann den Befehl **Ausführen** aus, um den IIS-Manager als Administrator auszuführen. Geben Sie an der Eingabeaufforderung folgenden Befehl ein:
runas /user:administrative_accountname "mmc%systemroot%\system32\inetsrv\iis.msc"

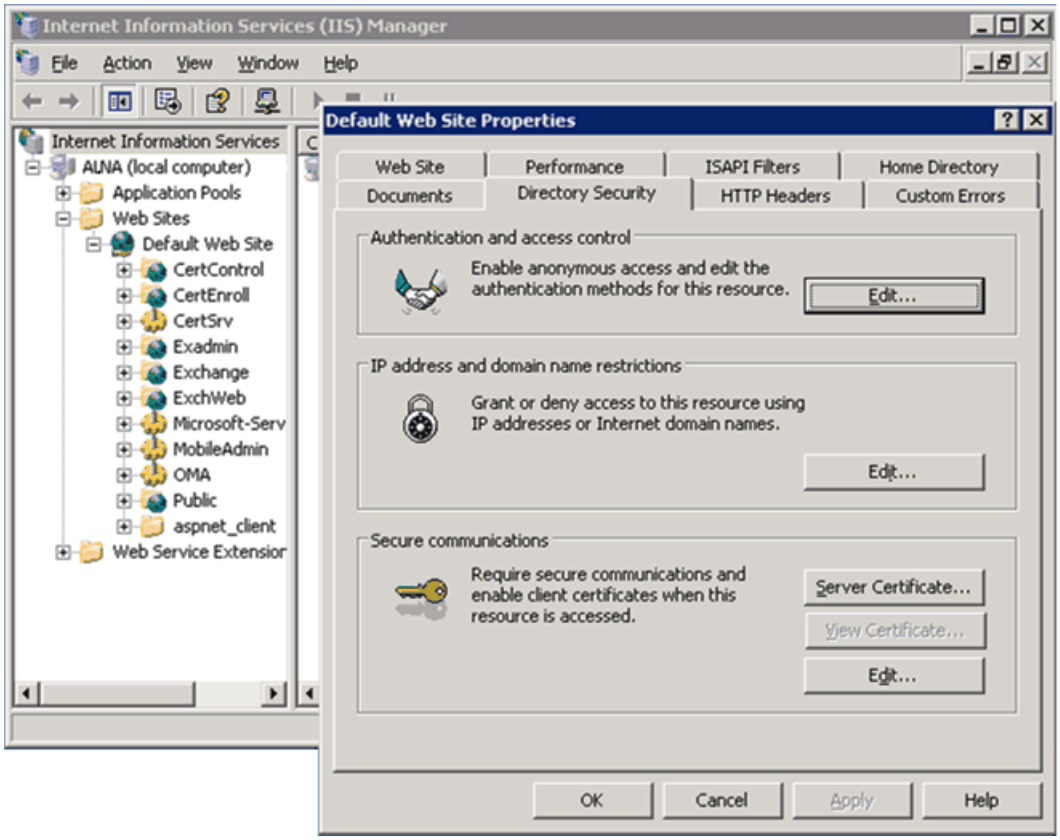
Anfordern und Installieren eines Serverzertifikats

Folgen Sie diesen Anweisungen, um ein Serverzertifikat anzufordern, zu installieren, die Installation zu überprüfen und das Zertifikat zu sichern. Wenn Sie zum Anfordern und Installieren eines Serverzertifikats den Assistenten für Webserverzertifikate verwenden, wird das Verfahren als Erstellen und Zuweisen eines Serverzertifikats bezeichnet.

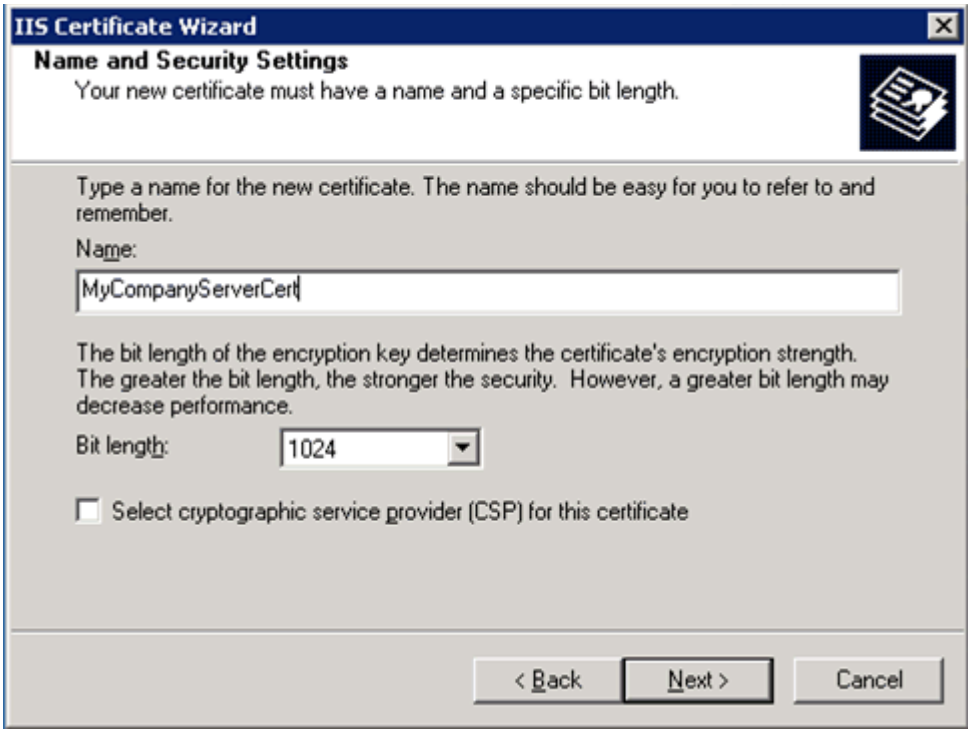
So fordern Sie ein Serverzertifikat von einer Zertifizierungsstelle an

1. Melden Sie sich mit einem Administratorkonto am Exchange-Server an.
2. Klicken Sie auf **Start**, klicken Sie auf **Programme**, klicken Sie auf **Verwaltung**, und klicken Sie dann auf **Internetinformationsdienste-Manager**.
3. Doppelklicken Sie auf den Servernamen, um die Websites anzuzeigen. Klicken Sie mit der rechten Maustaste auf **Standardwebsite**, und klicken Sie dann auf **Eigenschaften**.

4. Klicken Sie auf die Registerkarte **Verzeichnissicherheit**. Die folgende Abbildung zeigt das IIS-Manager-Fenster und die Registerkarte **Verzeichnissicherheit**. Klicken Sie unter **Sichere Kommunikation** auf **Serverzertifikat**.



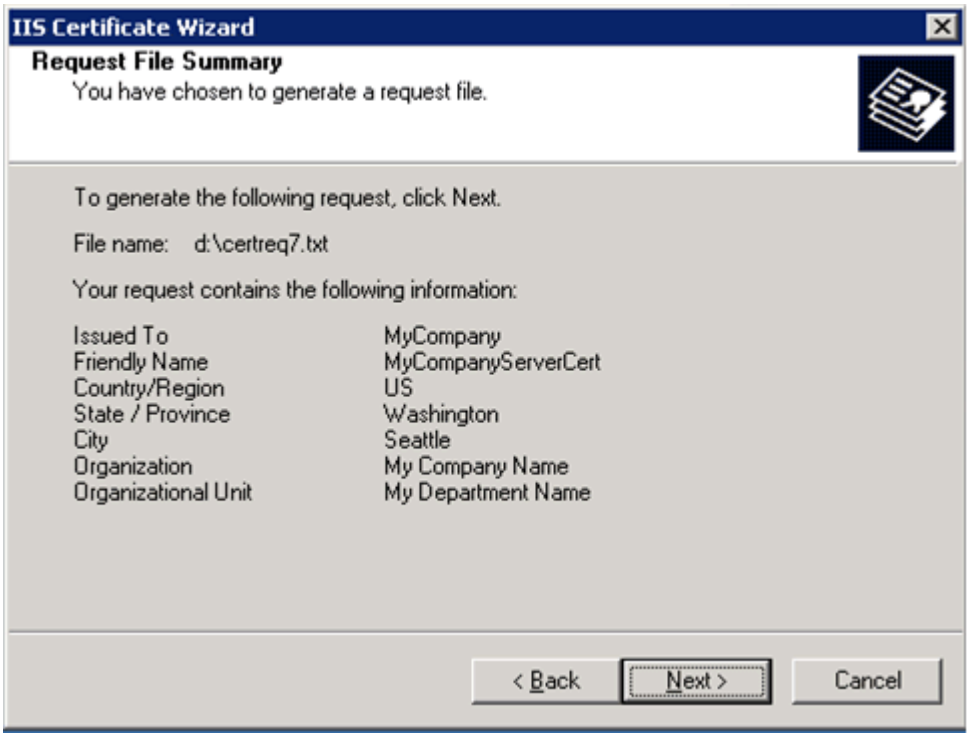
5. Klicken Sie im Dialogfeld **Willkommen** auf **Weiter**, klicken Sie auf **Neues Zertifikat erstellen**, und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf **Anforderung jetzt vorbereiten, aber später senden**, und klicken Sie dann auf **Weiter**.
7. Geben Sie im Dialogfeld **Name und Sicherheitseinstellungen** einen Namen für das Serverzertifikat ein (z. B. <Exchange_Server_Name>), übernehmen Sie **Bitlänge: 1024**, und klicken Sie dann auf **Weiter**. Die folgende Abbildung zeigt das Dialogfeld **Name und Sicherheitseinstellungen**.


IIS Certificate Wizard
Name and Security Settings
Your new certificate must have a name and a specific bit length.
Type a name for the new certificate. The name should be easy for you to refer to and remember.
Name:
MyCompanyServerCert
The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.
Bit length:
1024
Select cryptographic service provider (CSP) for this certificate
< Back
Next >
Cancel

Hinweis:

Stellen Sie sicher, dass **Kryptografiedienstanbieter (CSP) für dieses Zertifikat auswählen** deaktiviert ist.

8. Geben Sie im Dialogfeld **Information über Ihre Organisation** einen Namen in das Textfeld **Organisation** (z. B. <Firmenname>) und in das Textfeld **Organisationseinheit** ein (z. B. <IT-Abteilung>), und klicken Sie dann auf **Weiter**.
9. Geben Sie im Dialogfeld **Gemeinsamer Name (CN) der Site** den vollqualifizierten Domänennamen des Servers oder Clusters in das Feld **Gemeinsamer Name** ein (z. B. webmail.meinunternehmen.com>), und klicken Sie dann auf **Weiter**. Auf diesen Domänennamen greifen die mobilen Clientgeräte anschließend zu.
10. Klicken Sie im Dialogfeld **Geographische Informationen** auf **Land/Region** (z. B. US), **Bundesland/Kanton** (z. B. <Bundesland>) und **Ort** (z. B. <Stadt>), und klicken Sie dann auf **Weiter**.
11. Übernehmen Sie im Dialogfeld **Zertifikatanforderung *Dateiname*** den Standardeintrag **C:\NewKeyRq.txt** (wobei C: das Verzeichnis ist, in dem das Betriebssystem installiert ist), und klicken Sie dann auf **Weiter**.
12. Überprüfen Sie die Informationen im Dialogfeld **Zusammenfassung der Anforderungsdatei**, und klicken Sie dann auf **Weiter**. Die folgende Abbildung zeigt ein Beispiel für das Dialogfeld **Zusammenfassung der Anforderungsdatei**.



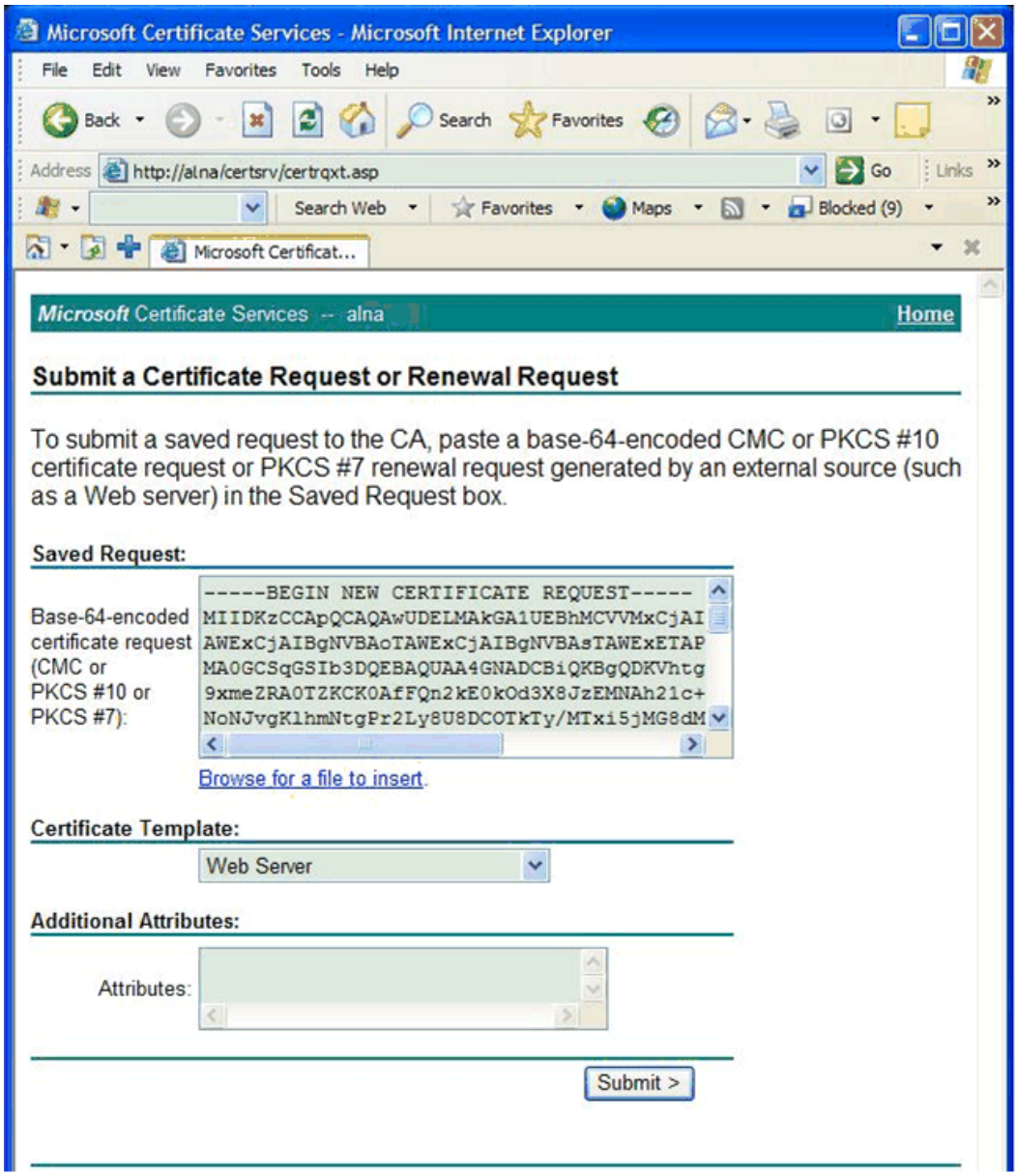
13. Nach Abschluss der Zertifikatanforderung wird eine entsprechende Meldung angezeigt. Klicken Sie auf **Fertig stellen**.

Als Nächstes müssen Sie ein Serverzertifikat von einer gültigen Zertifizierungsstelle anfordern. Dazu müssen Sie je nach der ausgewählten Zertifizierungsstelle auf das Internet oder ein Intranet zugreifen. Verwenden Sie dazu einen ordnungsgemäß konfigurierten Webbrowser.
Die hier aufgeführten Schritte betreffen den Zugriff auf die Website für Ihre Zertifizierungsstelle. In einer Produktionsumgebung fordern Sie vermutlich ein Serverzertifikat von einer vertrauenswürdigen Zertifizierungsstelle über das Internet an.

So senden Sie die Zertifikatanforderung

1. Starten Sie **Microsoft Internet Explorer®**. Geben Sie die URL (Uniform Resource Locator) für die Website der Microsoft-Zertifizierungsstelle, **http://<server_name>/certsrv/**, ein. Klicken Sie auf der Seite **Microsoft Zertifikatdienste** auf **Zertifikat anfordern**, und klicken Sie dann auf **Erweiterte Zertifikatanforderung**.
2. Klicken Sie auf der Seite **Erweiterte Zertifikatanforderung** auf **Reichen Sie eine Zertifikatanforderung ein, die eine Base64-codierte CMD- oder PKCS10-Datei verwendet, oder eine Erneuerungsanforderung, die eine Base64-codierte PKCS7-Datei verwendet**.
3. Wechseln Sie auf dem lokalen Server in das Verzeichnis der Datei **C:\NewKeyRq.txt**, die Sie zuvor gespeichert haben.
4. Doppelklicken Sie auf die Datei **C:\NewKeyRq.txt**, um sie im Editor zu öffnen. Wählen Sie den gesamten Inhalt der Datei aus, und kopieren Sie ihn.

5. Wechseln Sie auf der Website der Zertifizierungsstelle auf die Seite **Zertifikat- oder Erneuerungsanforderung einreichen**. Wenn Sie zur Auswahl des Zertifikattyps aufgefordert werden, klicken Sie auf **Webserver**. Die folgende Abbildung zeigt ein Beispiel für die Seite **Zertifikat- oder Erneuerungsanforderung einreichen**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://alna/certsrv/certrqxt.asp
Go Links
Search Web Favorites Maps Blocked (9)
Microsoft Certificat...
Microsoft Certificate Services -- alna
Home
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.
Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDKzCCApQCAQAwUDELMAkGA1UEBhMCVVMxCjAI
AWExCjAIBgNVBAoTAWExCjAIBgNVBAsTAWExETAP
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDKVhtg
9xmeZRA0TZKCK0AfFQn2kE0kOd3X8JzEMNAh21c+
NoNJvgKlhmNtgPr2Ly8U8DCOTkTy/MTxi5jMG8dM
Browse for a file to insert.
Certificate Template:
Web Server
Additional Attributes:
Attributes:
Submit >

6. Klicken Sie in das Feld **Gespeicherte Anforderung**, fügen Sie den Inhalt der Datei in das Feld ein, und klicken Sie dann auf **Einsenden**. Der Inhalt des Dialogfelds **Gespeicherte Anforderung** ähnelt dem folgenden Beispiel:

   -----BEGIN NEW CERTIFICATE REQUEST-----

   MIIDXzCCAsgCAQAwgYMxLDAqBgNVBAMTI2toYWxpZHM0LnJlZG1vbmQuY29ycC5
   taWNyb3NvZnQuY29tMREwDwYDVQQLEwhNb2JpbGl0eTEMMAoGA1UEChMDTVRQ
   MRAwDgYDVQQHEwdSZWRtb25kMRMwEQYDVQQIEwpXYXNoaW5ndG9uMQswCQ
   YDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAs0sV2UZ1WAX2
   ou+F5S34+6M3A32tJ5qp+c7zliu4SMkcgebhnt2IMMeF5ZMD2IqfhWu49nu1vLtGH
   K5wWgHYTC3rTFabLZJ1bNtXKB/BWWOsmSDYg/A7+oCZB4rHJmpc0Yh4OjbQKkr6
   4KM67r8jGEPYGMAzf2DnUg3xUt9pbBECAwEAAaCCAZkwGgYKKwYBBAGCNw0CAz
   EMFgo1LjAuMjE5NS4yMHsGCisGAQQBgjcCAQ4xbTBrMA4GA1UdDwEB/wQEAwIE8
   DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAI
   CAIAwBwYFKw4DAgcwCgYIKoZIhvcNAwcwEwYDVR0lBAwwCgYIKwYBBQUHAwEw
   gf0GCisGAQQBgjcNAgIxge4wgesCAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFI
   AUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcA
   BoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgOBiQCO5g/Nk+lsuAJZideg15faBLqe4jiiy
   tYeVBApxLrtUlyWEQuWdPeEFv0GWvsjQGwn+WC5m9kVNmcLVsx41QtGDXtuETFO
   D6dSi/M9wmEy8bsbcNHXs+sntX56AcCxBXh1ALaE4YaE6e/zwmE/0/Cmyje3a2olE
   5rlk1FFIlKTDwAAAAAAAAAAMA0GCSqGSIb3DQEBBQUAA4GBAAr7zjg2ykZoFUYt1
   +EgK106jRsLxJcoqj0oEg575eAlUgbN1e2i/L2RWju7cgo9W7uwwpBIaEqd6LJ6s1BR
   pZz0yeJTDzGIXByG5O6kouk+0H+WHCj2yI30zik8aSyCQ3rQbNvHoURDmWqv9Rp
   1BDC1SNQLEzDgZjKPrsGZAVLb

   -----END NEW CERTIFICATE REQUEST-----

7. Klicken Sie auf der Seite **Zertifikat wurde ausgestellt** auf **DER-codiert**, und klicken Sie dann auf **Download des Zertifikats**.
8. Klicken Sie im Dialogfeld **Dateidownload** auf **Datei auf Datenträger speichern**, und klicken Sie dann auf **OK**. Übernehmen Sie die Standardeinstellung, um die Datei auf dem Desktop zu speichern, und klicken Sie dann auf **Speichern**.
9. Schließen Sie Internet Explorer.

An dieser Stelle ist auf Ihrem Desktop ein Serverzertifikat vorhanden, das in den Zertifikatsspeicher von Exchange Server importiert werden kann. Als Nächstes müssen Sie das Zertifikat installieren.

So installieren Sie das Serverzertifikat

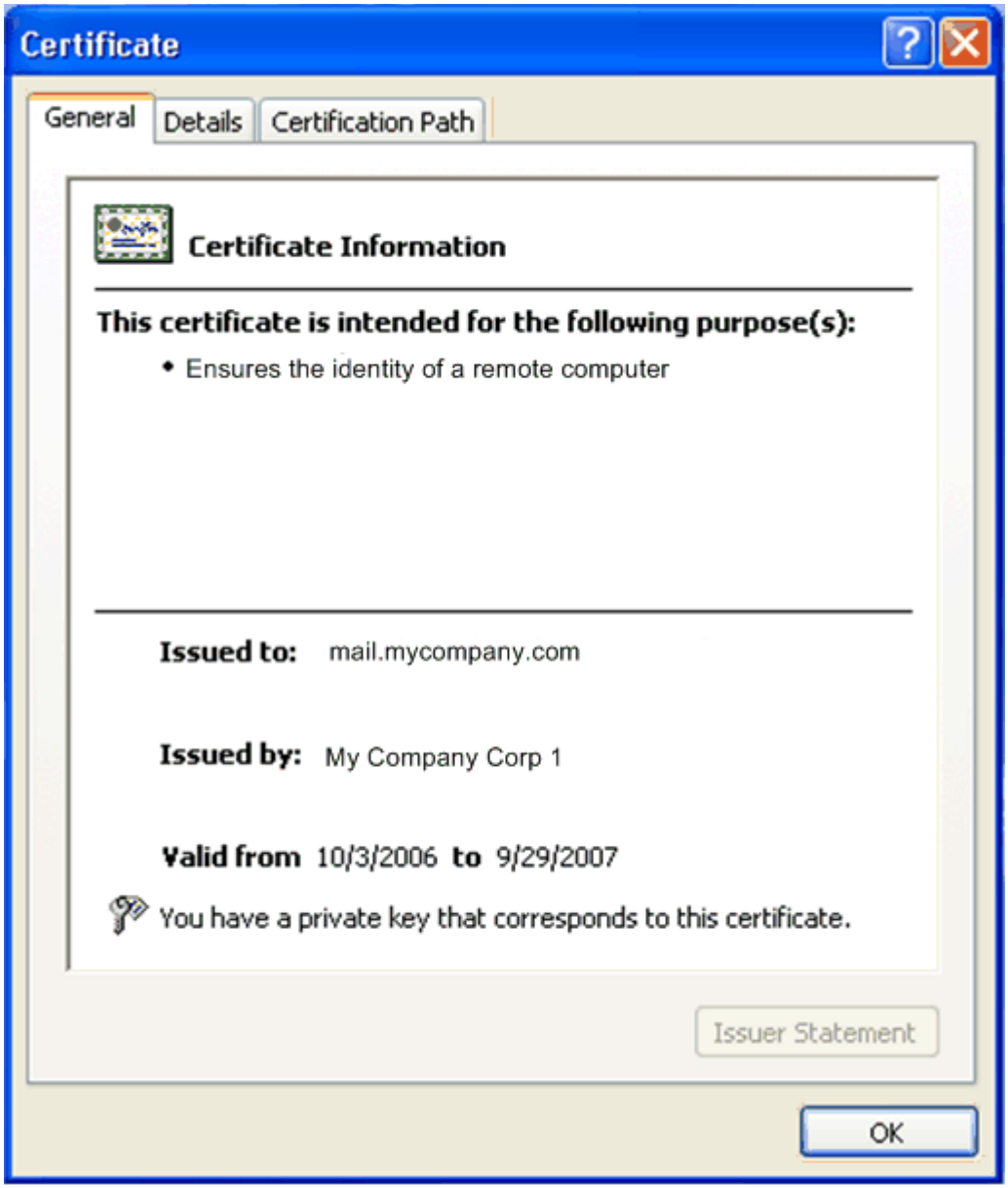
1. Starten Sie **Internetinformationsdienste-Manager**, und erweitern Sie <Domänenname>
2. Klicken Sie mit der rechten Maustaste auf **Standardwebsite**, und klicken Sie dann auf **Eigenschaften**. Klicken Sie im Dialogfeld **Eigenschaften** auf die Registerkarte **Verzeichnissicherheit**. Klicken Sie unter **Sichere Kommunikation** auf **Serverzertifikat**.
3. Klicken Sie im Dialogfeld **IIS-Zertifikat-Assistent** auf **Weiter**.
4. Aktivieren Sie **Ausstehende Anforderung verarbeiten und Zertifikat installieren**. Klicken Sie auf **Weiter**.
5. Wechseln Sie in das Verzeichnis und zu der Datei (oder geben Sie den Pfad ein), die das Serverzertifikat **certnew.txt** auf dem Desktop enthält, und klicken Sie dann auf **Weiter**.
6. Wählen Sie den SSL-Port aus, den Sie verwenden möchten. Es wird empfohlen, den SSL-Standardport **Port 443** zu verwenden.
7. Klicken Sie im Dialogfeld **Zertifikatzusammenfassung** auf **Weiter**, und klicken Sie dann auf **Fertig stellen**.

Überprüfen der Installation

Zeigen Sie das Serverzertifikat an, um die Installation zu überprüfen.

So zeigen Sie das Serverzertifikat an

1. Klicken Sie im Dialogfeld **Eigenschaften von Standardwebsite** auf **Verzeichnissicherheit**. Klicken Sie unter **Sichere Kommunikation** auf **Zertifikat anzeigen**. Die folgende Abbildung zeigt das Dialogfeld **Zertifikat**.



2. Unten im Dialogfeld **Zertifikat** gibt eine Meldung gegebenenfalls an, dass ein privater Schlüssel installiert ist. Klicken Sie auf **OK**, um das Dialogfeld **Zertifikat** zu schließen.

Hinweis:

Wenn das Zertifikat nicht zeigt, dass das Gerät über den privaten Schlüssel verfügt, der dem Zertifikat entspricht, funktioniert keine Synchronisierung über das Funknetzwerk.

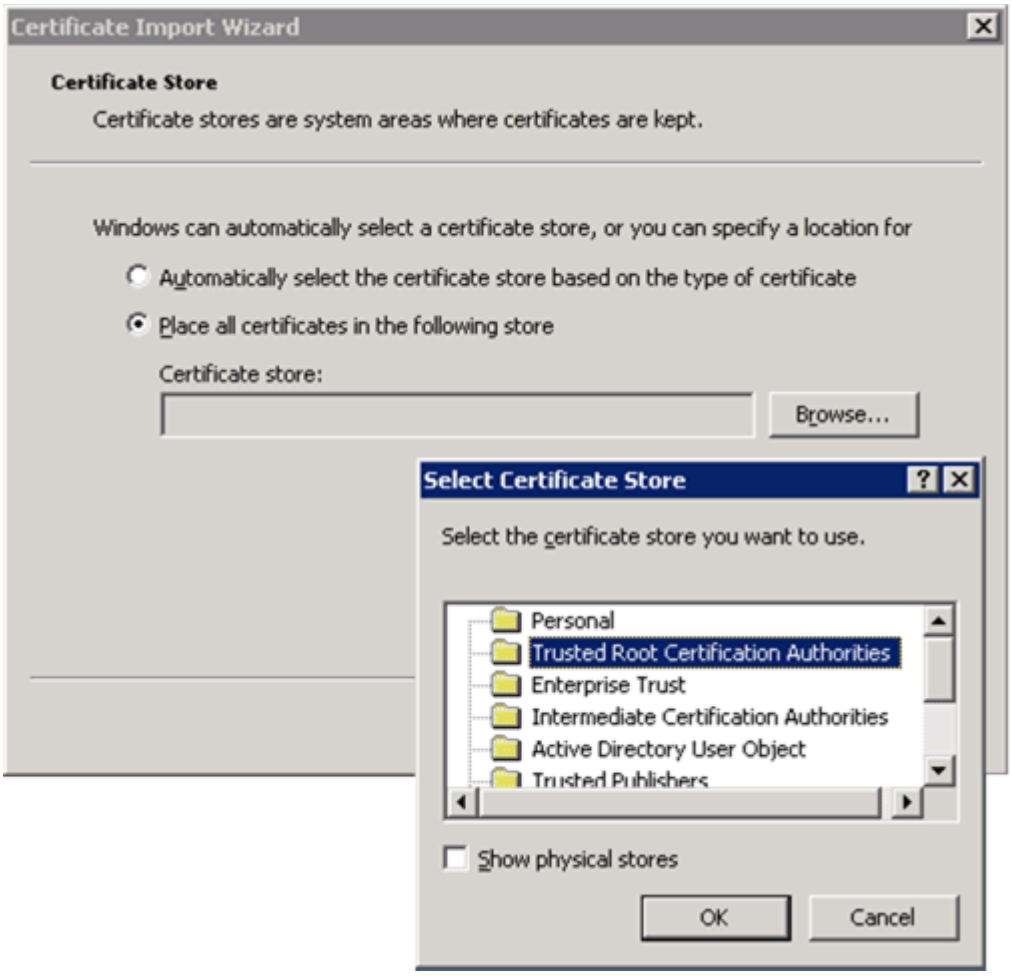
Damit die Authentifizierung funktioniert, müssen Sie die Zertifizierungsstelle der Liste vertrauenswürdiger Stammzertifizierungsstellen hinzufügen.

So fügen Sie die Zertifizierungsstelle der Liste der vertrauenswürdigen Stammzertifizierungsstellen hinzu

1. Starten Sie **Internet Explorer**, und geben Sie dann die URL für Ihre Zertifizierungsstelle ein. Wenn Sie z. B. das Serverzertifikat von der zuvor konfigurierten Zertifizierungsstelle erhalten haben, geben Sie **http://<server_name>/certsrv** ein.
2. Klicken Sie auf **Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Zertifikatsperrliste**, und klicken Sie dann auf der nächsten Seite auf **Download des Zertifizierungsstellenzertifikats**. Klicken Sie im Dialogfeld **Dateidownload** auf **Datei auf Datenträger speichern**, und klicken Sie dann auf **OK**.
3. Geben Sie ein Serverzertifikat in das Feld **Name** ein (z. B. <certnewca.cer>), und speichern Sie die Datei dann auf dem Desktop.
4. Wechseln Sie zum Desktop. Klicken Sie mit der rechten Maustaste auf die Datei, die Sie in Schritt 3 erstellt haben, und klicken Sie dann auf **Zertifikat installieren**. Klicken Sie im Dialogfeld **IIS-Zertifikat-Assistent** auf **Weiter**.
5. Klicken Sie auf **Alle Zertifikate in folgendem Speicher speichern**, und klicken Sie dann auf **Durchsuchen**. Wählen Sie den Ordner **Vertrauenswürdige Stammzertifizierungsstellen** aus, und klicken Sie dann auf **OK**. Die folgende Abbildung zeigt das Dialogfeld **Zertifikatspeicher auswählen**.

Hinweis:

Sie können anstelle von **Vertrauenswürdige Stammzertifizierungsstellen** auch **Zwischenzertifizierungsstellen** verwenden.


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Show physical stores
OK
Cancel

6. Klicken Sie auf **Weiter**. Ein Dialogfeld wird mit dem Hinweis angezeigt, dass das Zertifikat einem vertrauenswürdigen Zertifikatspeicher hinzugefügt wird. Klicken Sie auf **Ja**, um das Dialogfeld zu schließen. Klicken Sie auf **Fertig stellen**. Anschließend wird eine Meldung angezeigt, dass der Import erfolgreich war.

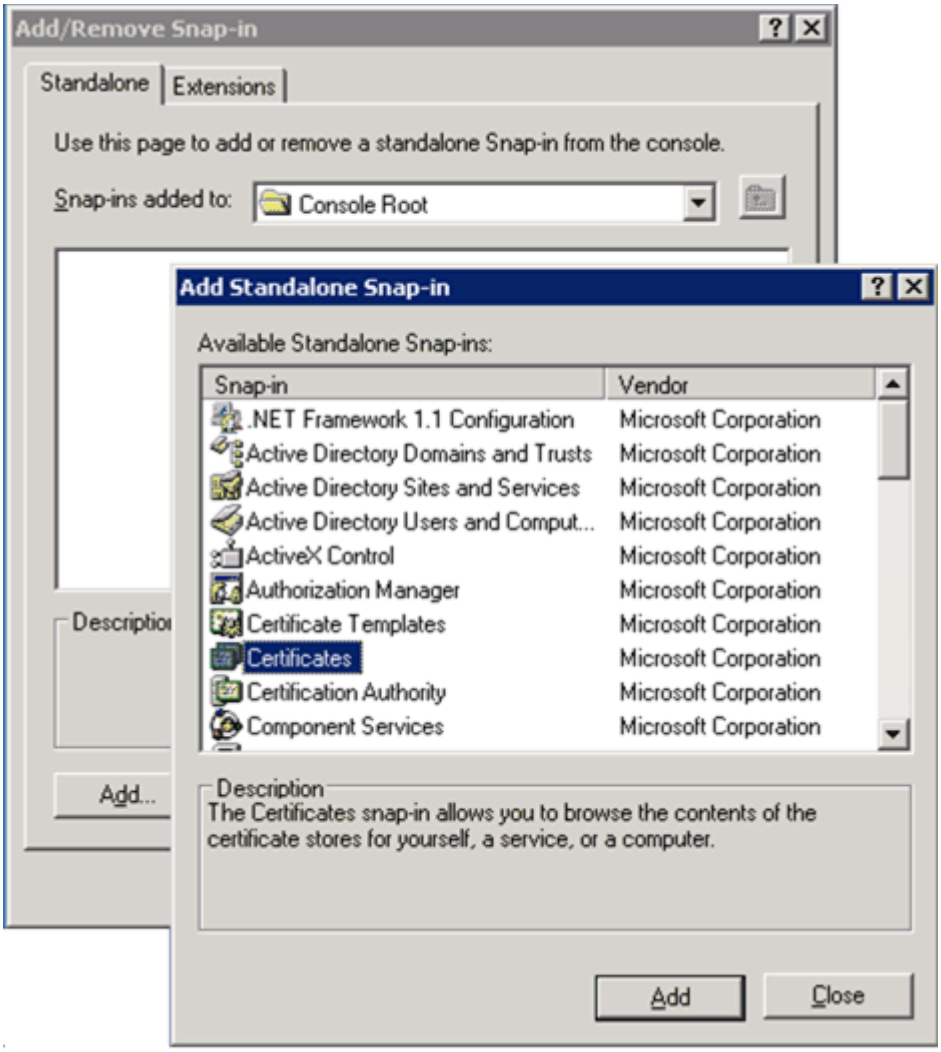
Sichern des Serverzertifikats

Sie können die Serverzertifikate mithilfe des Assistenten für Webserverzertifikate sichern. Aufgrund der engen Integration von IIS in Windows können Sie die Zertifikatverwaltung, die in Microsoft Management Console (MMC) **Zertifikate** genannt wird, zum Exportieren und Sichern von Serverzertifikaten verwenden.

Wenn Sie die Zertifikatverwaltung in MMC nicht installiert haben, müssen Sie die Zertifikatverwaltung MMC hinzufügen.

So fügen Sie die Zertifikatverwaltung MMC hinzu

1. Klicken Sie im Menü **Start** auf **Ausführen**.
2. Geben Sie **mmc** in das Feld **Öffnen** ein, und klicken Sie dann auf **OK**.
3. Klicken Sie im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
4. Klicken Sie im Dialogfeld **Snap-In hinzufügen/entfernen** auf **Hinzufügen**.
5. Die folgende Abbildung zeigt die Dialogfelder **Snap-In hinzufügen/entfernen** und **Eigenständiges Snap-In hinzufügen**. Klicken Sie in der Liste **Verfügbare eigenständige Snap-Ins** auf **Zertifikate**, und klicken Sie dann auf **Hinzufügen**.



6. Klicken Sie auf **Computerkonto**, und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf **Lokaler Computer** (der Computer, auf dem die Konsole ausgeführt wird), und klicken Sie dann auf **Fertig stellen**.
8. Klicken Sie auf **Schließen**, und klicken Sie dann auf **OK**.

Wenn die Zertifikatverwaltung installiert ist, können Sie das Serverzertifikat sichern.

So sichern Sie das Serverzertifikat

1. Suchen Sie den richtigen Zertifikatspeicher. Der Speicher befindet sich in der Regel im Speicher **Lokaler Computer** der Zertifikatverwaltung.

   Hinweis:

   Wenn die Zertifikatverwaltung installiert ist, wird auf den richtigen Zertifikatspeicher **Lokaler Computer** verwiesen.
2. Klicken Sie im Ordner **Eigene Zertifikate** auf das Serverzertifikat, das Sie sichern möchten.
3. Zeigen Sie im Menü **Aktion** auf **Alle Aufgaben**, und klicken Sie dann auf **Exportieren**.
4. Klicken Sie im Dialogfeld **Zertifikatexport-Assistent** auf **Ja, privaten Schlüssel exportieren**.
5. Übernehmen Sie die Standardeinstellungen des Assistenten, und geben Sie ein Kennwort für die Sicherungsdatei des Serverzertifikats ein, wenn Sie dazu aufgefordert werden.

   Hinweis:

   Aktivieren Sie nicht **Privaten Schlüssel nach erfolgreichem Export löschen**, da diese Option das aktuelle Serverzertifikat deaktiviert.
6. Führen Sie den Assistenten vollständig aus, um eine Sicherungskopie des Serverzertifikats zu exportieren.

Nachdem Sie das Netzwerk zum Erstellen von Zertifikaten konfiguriert haben, müssen Sie den Exchange-Clientzugriffsserver und seine Dienste aktualisieren. Legen Sie dazu fest, dass die Kommunikation mit dem Clientzugriffsserver über SSL erfolgen muss. Im folgenden Abschnitt wird beschrieben, wie SSL für die Standardwebsite aktiviert wird.

Aktivieren von SSL für die Standardwebsite

Sie haben ein SSL-Zertifikat angefordert, das vom Exchange-Clientzugriffsserver entweder auf der Standardwebsite oder auf der Website verwendet wird, auf der Sie die virtuellen Verzeichnisse **\Exchange**, **\Exchweb**, **\Microsoft-Server-ActiveSync** und **\Public** bereitstellen. Anschließend können Sie für die Standardwebsite festlegen, dass die Verwendung von SSL erforderlich ist.

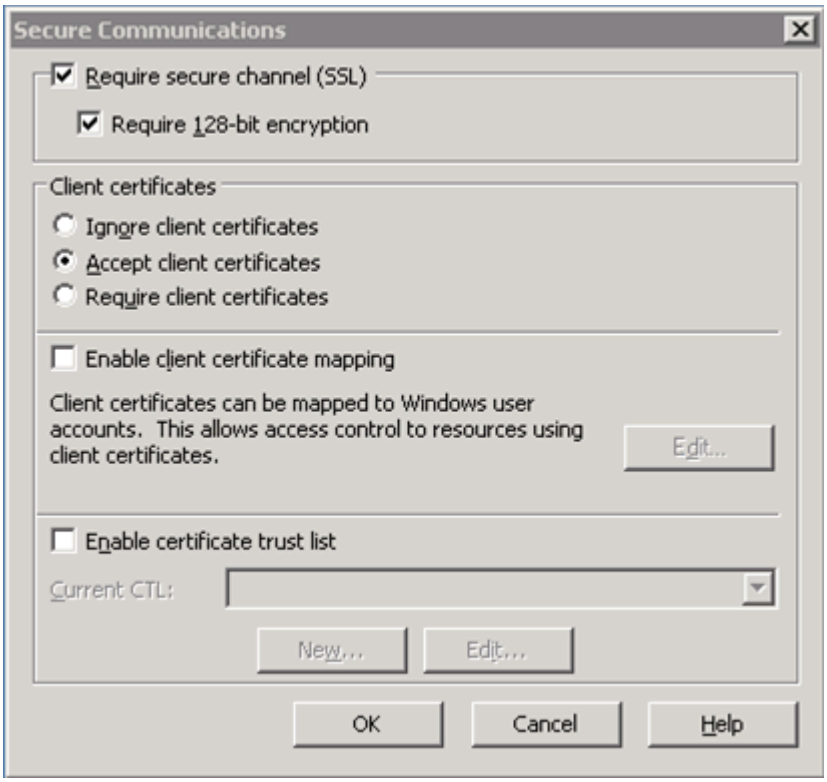
Hinweis:

Die virtuellen Verzeichnisse **\Exchange**, **\Exchweb**, **\Microsoft-Server-ActiveSync** und **\Public** werden bei jeder Installation von Exchange Server 2007 standardmäßig installiert. Das virtuelle Verzeichnis **\RPC** für die RPC-über-HTTP-Kommunikation wird manuell installiert, wenn Sie Exchange Server 2007 für die Unterstützung von RPC-über-HTTP konfigurieren.

So legen Sie die Verwendung von SSL für die Standardwebsite fest

1. Aktivieren Sie in **Internetinformationsdienste-Manager** die Standardwebsite oder die Website, auf der Sie die Exchange Server 2007-Dienste bereitstellen, und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie im Dialogfeld **Sichere Kommunikation** auf der Registerkarte **Verzeichnissicherheit** auf **Bearbeiten**.

3. Die folgende Abbildung zeigt das Dialogfeld **Sichere Kommunikation**. Aktivieren Sie das Kontrollkästchen **Sicheren Kanal voraussetzen (SSL)**. Klicken Sie auf **OK**.



4. Abhängig von Ihrer Installation wird möglicherweise das Dialogfeld **Vererbungsüberschreibungen** angezeigt. Wählen Sie die virtuellen Verzeichnisse aus, die die neue Einstellung erben sollen, z. B. Microsoft-Server-ActiveSync, und klicken Sie dann auf **OK**.
5. Klicken Sie auf der Registerkarte **Verzeichnissicherheit** auf **OK**.

Nachdem Sie dieses Verfahren ausgeführt haben, sind die virtuellen Verzeichnisse auf dem Exchange-Clientzugriffsserver, der sich auf der Standardwebsite befindet, für die Verwendung von SSL konfiguriert.

Konfigurieren der Standardauthentifizierung

Die Exchange ActiveSync-Website unterstützt SSL-Verbindungen, sobald das Serverzertifikat an die Website gebunden ist. Die Benutzer haben jedoch noch immer die Option, eine nicht sichere Verbindung mit der Exchange ActiveSync-Website herzustellen. Sie können festlegen, dass alle Windows Mobile 6-basierten Geräte zuerst eine SSL-Verbindung herstellen, bevor sie mit den Verzeichnissen der Exchange ActiveSync-Website verbunden werden.

Es wird empfohlen, dass Sie die Standardauthentifizierung für alle HTTP-Verzeichnisse erzwingen, die ISA Server für externe Benutzer zugänglich macht. Auf diese Weise können Sie das Feature von ISA Server nutzen, mit dem die Anmeldeinformationen der Standardauthentifizierung von der Firewall an die Exchange ActiveSync-Website weitergeleitet werden können.

Festlegen einer SSL-Verbindung mit den Verzeichnissen der Exchange ActiveSync-Website

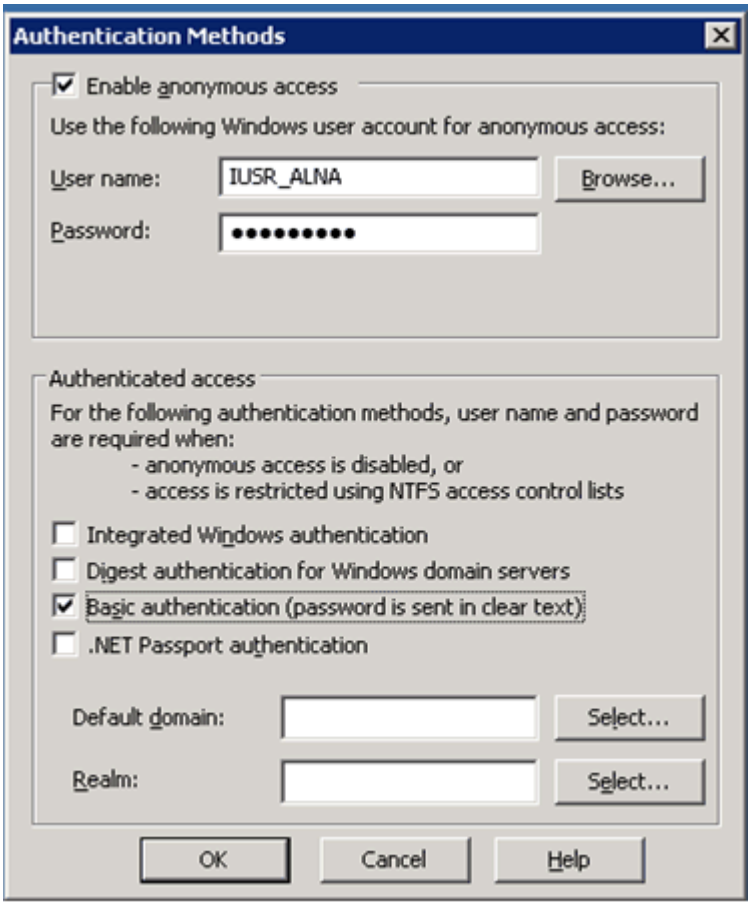
Dieses Verfahren trägt dazu bei, nicht authentifizierte Verbindungen mit der Exchange ActiveSync-Website zu verhindern.

Sie können diese Schritte mit den Verzeichnissen **/Exchange**, **/Exchweb** und **/Public** wiederholen, die sich im linken Bereich des MMC-Konsolenfensters von IIS befinden. Damit legen Sie fest, dass SSL für die vier Websiteverzeichnisse verwendet werden muss, die Sie für Remotebenutzer zugänglich machen können:

- /Exchange
- /ExchWeb
- /Microsoft-Server-ActiveSync
- /Public

So legen Sie die Verwendung einer SSL-Verbindung mit den Verzeichnissen der Exchange ActiveSync-Website fest

1. Klicken Sie auf **Start**, klicken Sie auf **Verwaltung**, und klicken Sie dann auf **Internetinformationsdienste-Manager**. Erweitern Sie in **Internetinformationsdienste-Manager** den Servernamen, und erweitern Sie dann im linken Bereich der Konsole den Knoten **Standardwebsite**.
2. Klicken Sie mit der rechten Maustaste auf das Verzeichnis **Microsoft-Server-ActiveSync**, um es hervorzuheben, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf **Verzeichnissicherheit**. Klicken Sie im Abschnitt **Authentifizierung und Zugriffssteuerung** auf **Bearbeiten**.
4. Die folgende Abbildung zeigt das Dialogfeld **Authentifizierungsmethoden**. Deaktivieren Sie alle Kontrollkästchen außer **Standardauthentifizierung** (das Kennwort wird als Klartext gesendet). Aktivieren Sie das Kontrollkästchen **Standardauthentifizierung**.



5. Klicken Sie in dem Dialogfeld mit dem Hinweis, dass die Anmeldeinformationen mit SSL geschützt werden sollten, auf **Ja**. Geben Sie in das Textfeld **Standarddomäne** den Namen Ihrer Domäne ein.
6. Klicken Sie auf **OK**.
7. Klicken Sie im Dialogfeld **Exchange Eigenschaften** auf **Übernehmen**, und klicken Sie dann auf **OK**.
8. Schließen Sie die Konsole **Internetinformationsdienste-Manager**, nachdem Sie die Standardauthentifizierung für die von Ihnen ausgewählten Verzeichnisse festgelegt haben.

Konfigurieren oder Aktualisieren von Update RSA SecurID Agent (Optional)

Richten Sie Exchange-Server möglichst als Agent-Host in der RSA ACE/Server-Datenbank ein, wenn Sie RSA SecurID als zusätzliche Sicherheitsschicht verwenden.

Hinweis:

Es gibt zeitliche Abweichungen zwischen IIS 6.0 und dem RSA ACE/Agent. Aktualisieren Sie den RSA ACE/Agent, um die Kompatibilität mit IIS 6.0 zu erhöhen. Weitere Informationen finden Sie auf der Website von RSA Security.

Schützen von IIS durch eine Verringerung potenzieller Angriffsflächen

Schützen Sie IIS, indem Sie alle Features und Dienste deaktivieren, die nicht direkt benötigt werden. Lassen Sie erst dann den Zugriff auf Ihre Server über das Internet zu.

- In Windows Server 2003 werden IIS-Features standardmäßig deaktiviert, um die Sicherheit zu erhöhen.
- In Microsoft Windows Server 2000 können Sie IIS besser schützen, indem Sie den IIS-Sicherheits-Assistenten und das UrlScan-Tool herunterladen und ausführen (wie im Folgenden beschrieben).

Windows Server 2003 SP2 und IIS 6.0

IIS 6.0 wird durch viele integrierte Features von Microsoft Windows Server 2003 geschützt. Zum Schutz vor böswilligen Benutzern und Angreifern schließt die Standardkonfiguration für Produkte der Windows Server 2003-Produktfamilie IIS nicht ein. IIS wird bei der Installation in einem äußerst sicheren „Sperrmodus“ konfiguriert, der nur statischen Inhalt zulässt. Sie können die ISS-Funktionen mithilfe der Webdiensterweiterungen den speziellen Anforderungen Ihrer Organisation entsprechend aktivieren oder deaktivieren.

Weitere Informationen finden Sie im Abschnitt zum Verringern der Angriffsflächen auf den Webserver (IIS 6.0) im Bereitstellungshandbuch zu IIS unter http://go.microsoft.com/fwlink/?LinkId=67608 (möglicherweise in englischer Sprache).

Verwendung von UrlScan

UrlScan, Version 2.5, ist ein Sicherheitstool, mit dem die von Internetinformationsdienste (IIS) verarbeiteten HTTP-Anforderungstypen eingeschränkt werden können. Indem bestimmte HTTP-Anforderungen blockiert werden, verhindert das UrlScan-Sicherheitstool, dass schädliche Anforderungen den Server erreichen. UrlScan 2.5 wird nun als eigenständige Installation auf Servern mit Microsoft IIS 4.0 oder höher implementiert.

UrlScan 2.5 ist kein Bestandteil von IIS 6.0, da integrierte Features von IIS 6.0 eine ähnliche oder bessere Sicherheitsfunktionalität bieten als die meisten Features von UrlScan 2.5. UrlScan besitzt jedoch einige zusätzliche Funktionen (z. B. Verbkontrolle), die in IIS 6.0 nicht enthalten sind. Wenn Sie das UrlScan-Sicherheitstool in Ihre Serververwaltungsmethoden integriert haben, sind für Sie die zusätzlichen Funktionen und Features von UrlScan 2.5 sicher nützlich.

Wenn Sie das UrlScan-Tool herunterladen möchten, besuchen Sie die Website zum Sicherheitstool UrlScan unter http://go.microsoft.com/fwlink/?LinkID=89648&clcid=0x409 (möglicherweise in englischer Sprache).

Weitere Informationen zu UrlScan und über IIS 6.0 hinausgehende Funktionen finden Sie im Abschnitt zu dem Thema, ob UrlScan 2.5 mit IIS 6.0 eingesetzt werden soll, auf der Website zum Sicherheitstool UrlScan.

Schritt 4: Installieren und Konfigurieren von ISA Server 2006 oder einer anderen Firewall

Microsoft Internet Security and Acceleration (ISA) Server 2006 und Microsoft Exchange Server 2007 arbeiten in Ihrem Netzwerk eng zusammen und sorgen für eine sichere Mobile Messaging-Umgebung.

ISA Server 2006 ist das Sicherheitsgateway, das Ihre Anwendungen vor Gefahren aus dem Internet schützt. ISA Server erweitert die Möglichkeiten Ihres Unternehmens, indem es einen sicheren Zugriff auf Microsoft-Anwendungen und -daten bietet.

Die von Microsoft empfohlene Topologie für eine Mobile Messaging-Umgebung besteht in der Kombination aus ISA Server 2006 und Exchange Server 2007. Lesen Sie vor der Installation von ISA Server 2006 die folgenden Artikel:

Dokumentation zu ISA Server 2006
Veröffentlichen von Exchange Server 2007 mit ISA Server 2006 http://go.microsoft.com/fwlink/?LinkID=87060&clcid=0x409 (möglicherweise in englischer Sprache)
Bewährte Methoden für die Leistungsoptimierung in ISA Server 2006 http://go.microsoft.com/fwlink/?LinkID=87155&clcid=0x409 (möglicherweise in englischer Sprache)
ISA Server 2006 Enterprise Edition Installationshandbuch http://go.microsoft.com/fwlink/?LinkID=87158&clcid=0x409 (möglicherweise in englischer Sprache)
ISA Server 2006 Standard Edition Installationshandbuch http://go.microsoft.com/fwlink/?LinkID=87159&clcid=0x409 (möglicherweise in englischer Sprache)
Authentifizierung in ISA Server 2006 http://go.microsoft.com/fwlink/?LinkID=87068&clcid=0x409 (möglicherweise in englischer Sprache)
Bewährte Methoden für Firewallrichtlinien in ISA Server 2006 http://go.microsoft.com/fwlink/?LinkID=87160&clcid=0x409 (möglicherweise in englischer Sprache)

Hinweis:

Wenn eine Firewall eines Drittanbieters verwendet wird, muss als weiterer Schritt lediglich das Zeitlimit für Leerlaufsitzungen für alle Firewalls und Netzwerkgeräte auf 1800 Sekunden (30 Minuten) festgelegt werden. Informationen zur entsprechenden Vorgehensweise finden Sie in der Dokumentation des Herstellers. Weitere Informationen zu den bewährten Direct Push-Methoden für die Firewall finden Sie unter Grundlegendes zu Direct Push.

Verfahren

- Dieser Teil des Prozesses umfasst Folgendes:
- Installieren von ISA Server 2006
- Installieren eines Serverzertifikats auf dem Computer mit ISA Server
- Aktualisieren öffentlicher DNS-Server
- Erstellen der Exchange ActiveSync-Webveröffentlichungsregel mithilfe der Webveröffentlichung

Hinweis:

Das Erstellen einer Exchange ActiveSync-Veröffentlichungsregel und eines Weblisteners wird durch ein Update für ISA Server 2006 vereinfacht. Dieses Update erhalten Sie unter http://go.microsoft.com/fwlink/?LinkID=87161&clcid=0x409.

- Konfigurieren von ISA Server mit dem LDAP- (Active Directory) oder RADIUS-Serversatz

  Hinweis:

  Dieser Schritt ist nur erforderlich, wenn ISA Server kein Domänenmitglied ist. RADIUS unterstützt außerdem keine Zuordnung von Benutzern zu Gruppen.

- Festlegen des Zeitlimits für Leerlaufsitzungen aller Firewalls und Proxyserver auf 1800 Sekunden (30 Minuten)

  Hinweis:

  Eine Erhöhung der Zeitlimits maximiert die Leistung der Direct Push-Technologie und optimiert die Batterielebensdauer von Geräten. Der Standardwert für alle ISA Server 2006-Weblistener beträgt 1800 Sekunden (30 Minuten).

- Testen von Outlook Web Access (OWA) und Exchange ActiveSync

Installieren von ISA Server 2006

Wichtig:

Lesen Sie vor der Installation von ISA Server 2006 unbedingt das Installationshandbuch zu ISA Server 2006 Enterprise Edition oder ISA Server 2006 Standard Edition, je nachdem, welche Version Sie installieren.

So installieren Sie ISA Server 2006

1. Installieren und konfigurieren Sie Microsoft Windows Server 2003 auf dem Firewallcomputer.
2. Wechseln Sie zu Microsoft Update, und installieren Sie alle wichtigen Sicherheitshotfixes und Service Packs für Windows Server 2003.
3. Installieren Sie ISA Server 2006.

   Wichtig:

   Überlegungen zur Installation von ISA Server 2006 in einer Arbeitsgruppe oder zu einer Domäne gehörend finden Sie unter Szenarien der Netzwerkarchitektur. Lesen Sie diese Szenarien, bevor Sie ISA Server 2006 in einer Arbeitsgruppe oder Domäne installieren. Ihre letztendliche Implementierungsstrategie sollte den Sicherheits- und Leistungsanforderungen Ihres Netzwerks entsprechen.
4. Wechseln Sie zu Microsoft Update, und installieren Sie alle wichtigen Sicherheitshotfixes und Service Packs für Windows Server 2006.
5. Exportieren Sie das OWA-SSL-Zertifikat vom Exchange-Clientzugriffsserver in eine Datei.

Installieren eines Serverzertifikats auf dem Computer mit ISA Server

Installieren Sie ein Serverzertifikat auf dem Computer mit ISA Server, um eine sichere Kommunikation zwischen mobilen Geräten und dem Computer mit ISA Server zu ermöglichen. Dieses Zertifikat sollte von einer öffentlichen Zertifizierungsstelle ausgestellt werden, da Benutzer aus dem Internet darauf zugreifen. Wenn Sie eine private Zertifizierungsstelle verwenden, muss das Stammzertifikat der Zertifizierungsstelle auf allen Computern, die eine sichere Verbindung (HTTPS) mit einem Computer mit ISA Server herstellen müssen, sowie im Speicher des lokalen Computers mit ISA Server installiert werden.

Führen Sie die folgenden Verfahren auf jedem Server aus, auf dem IIS installiert ist. Verwenden Sie diese Verfahren, um ein Zertifikat auf den Computer mit ISA Server zu importieren.

In diesem Abschnitt wird Folgendes beschrieben:

- Anfordern und Installieren eines Serverzertifikats von einer öffentlichen Zertifizierungsstelle
- Exportieren des Serverzertifikats in eine Datei
- Importieren des Serverzertifikats auf dem Computer mit ISA Server

Hinweis:

Eine Liste öffentlicher Zertifikatanbieter finden Sie unter Schritt 6: Zertifikatregistrierung und Geräteprovisioning.

Anfordern und Installieren eines Serverzertifikats von einer öffentlichen Zertifizierungsstelle

Führen Sie die folgenden Schritte aus, um ein Serverzertifikat anzufordern und auf einem Computer mit IIS zu installieren.

So fordern Sie ein Serverzertifikat von einer öffentlichen Zertifizierungsstelle an und installieren das Zertifikat

1. Erstellen Sie in IIS eine neue Website, die auf ein neues, leeres Verzeichnis verweist.
2. Erweitern Sie im IIS-Manager den lokalen Computer, klicken Sie mit der rechten Maustaste auf den Ordner **Websites**, klicken Sie auf **Neu**, und klicken Sie dann auf **Website**, um den Assistenten zum Erstellen einer Website zu starten.
3. Klicken Sie auf der Willkommenseite auf **Weiter**.
4. Geben Sie in das Feld **Beschreibung** einen Namen für die Website ein. Geben Sie z. B. **ISA-Zert-Site** ein, und klicken Sie dann auf **Weiter**.
5. Akzeptieren Sie die Standardeinstellungen auf der Seite **IP-Adresse und Porteinstellungen**.
6. Geben Sie auf der Seite **Basisverzeichnis der Website** einen Pfad für die Website ein. Beispiel: **c:\temp**.
7. Akzeptieren Sie die Standardeinstellungen auf der Seite **Zugriffsberechtigungen für die Website**, und klicken Sie auf **Weiter**.
8. Klicken Sie auf **Fertig stellen**, um den Assistenten zum Erstellen einer Website abzuschließen.

   Wichtig:

   Die neue Website wird standardmäßig beendet. Lassen Sie die Website beendet. Es gibt keinen Grund, die Website zu starten.

   Hinweis:

   Weitere Informationen zum Erstellen einer neuen Website finden Sie in der Dokumentation zu IIS.
9. Folgen Sie den Anweisungen der öffentlichen Zertifikatstelle, um mithilfe der in Schritt 1 erstellten Website ein Serverzertifikat zu erstellen und zu installieren.

   Wichtig:

   Die entscheidende Information im Zertifikat ist der gemeinsame Name bzw. der FQDN (Fully Qualified Domain Name, vollqualifizierte Domänenname). Geben Sie den FQDN ein, der von den Internetbenutzern verwendet wird, um die Verbindung mit der Exchange Outlook Web Access-Website herzustellen.

Hinweis:

Stellen Sie sicher, dass der private Schlüssel für das Zertifikat, das Sie installieren möchten, exportiert werden kann.

Exportieren des Serverzertifikats in eine Datei

Nachdem Sie das Zertifikat auf der von Ihnen erstellten Website installiert haben, exportieren Sie es in eine Datei. Anschließend kopieren Sie diese Datei und importieren sie auf den Computer mit ISA Server.

Führen Sie die folgenden Schritte aus, um das soeben installierte Serverzertifikat zu exportieren.

So exportieren Sie das Serverzertifikat in eine PFX-Datei

1. Erweitern Sie im IIS-Manager den lokalen Computer, und erweitern Sie dann den Ordner **Websites**.
2. Klicken Sie mit der rechten Maustaste auf **Website für Exchange-Front-End-Dienste**, klicken Sie auf **Standardwebsite**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Verzeichnissicherheit** unter **Sichere Kommunikation** auf **Serverzertifikat**, um den Assistenten für Webserverzertifikate zu starten.
4. Klicken Sie auf der Willkommenseite auf **Weiter**.
5. Aktivieren Sie **Aktuelles Zertifikat in eine PFX-Datei exportieren** auf der Seite **Aktuelle Zertifikatszuweisung ändern**.
6. Geben Sie auf der Seite **Zertifikat exportieren** den Pfad und den Dateinamen ein. Geben Sie z. B. **C:\Zertifikate\mail_isa.pfx** ein, und klicken Sie dann auf **Weiter**.
7. Geben Sie ein Kennwort für die PFX-Datei ein. Das Kennwort wird angefordert, wenn ein Benutzer eine PFX-Datei importiert. Die Verwendung eines sicheren Kennworts wird empfohlen, da die PFX-Datei auch den privaten Schlüssel enthält.

   Wichtig:

   Übertragen Sie die PFX-Datei mit einer sicheren Methode auf den Computer mit ISA Server. Die Datei enthält den privaten Schlüssel für das Zertifikat, das auf dem Computer mit ISA Server installiert werden soll.

Importieren des Serverzertifikats auf dem Computer mit ISA Server

Führen Sie auf dem Computer mit ISA Server die folgenden Schritte aus, um das Serverzertifikat in den Speicher des lokalen Computers zu importieren.

So importieren Sie ein Serverzertifikat auf dem Computer mit ISA Server

1. Kopieren Sie die im vorherigen Abschnitt erstellte PFX-Datei mit einer sicheren Methode auf den Computer mit ISA Server.
2. Klicken Sie auf **Start** und dann auf **Ausführen**. Geben Sie **mmc** in das Feld **Öffnen** ein, und klicken Sie dann auf **OK**.
3. Klicken Sie im Menü **Datei** auf **Snap-In hinzufügen/entfernen**. Klicken Sie dann im Dialogfeld **Snap-In hinzufügen/entfernen** auf **Hinzufügen**, um das Dialogfeld **Eigenständiges Snap-In hinzufügen** zu öffnen.

4. Wählen Sie **Zertifikate** aus, und klicken Sie auf **Hinzufügen**. Klicken Sie auf **Computerkonto**, und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf **Lokaler Computer**, und klicken Sie dann auf **Fertig stellen**. Klicken Sie im Dialogfeld **Eigenständiges Snap-In hinzufügen** auf **Schließen**, und klicken Sie dann im Dialogfeld **Snap-In hinzufügen/entfernen** auf **OK**.
6. Erweitern Sie den Knoten **Zertifikate**, and klicken Sie mit der rechten Maustaste auf den Ordner **Eigene Zertifikate**.
7. Wählen Sie **Alle Aufgaben,** und klicken Sie dann auf **Importieren**. Der Zertifikatimport-Assistent wird geöffnet.
8. Klicken Sie auf der Willkommenseite auf **Weiter**.
9. Suchen Sie auf der Seite **Importdateiname** die Datei, die Sie zuvor erstellt und auf den Computer mit ISA Server kopiert haben, und klicken Sie dann auf **Weiter**.
10. Geben Sie auf der Seite **Kennwort** das Kennwort für diese Datei ein, und klicken Sie dann auf **Weiter**.

    Hinweis:

    Die Seite **Kennwort** enthält die Option **Schlüssel als exportierbar markieren**. Wählen Sie diese Option nicht aus, wenn Sie das Exportieren des Schlüssels vom Computer mit ISA Server nicht zulassen möchten.
11. Stellen Sie auf der Seite **Zertifikatspeicher** sicher, dass **Alle Zertifikate in folgendem Speicher speichern** aktiviert und **Zertifikatspeicher** auf **Zertifikate automatisch registrieren** festgelegt ist, und klicken Sie dann auf **Weiter**.
12. Klicken Sie auf der letzen Seite des Assistenten auf **Fertig stellen**.
13. Überprüfen Sie, ob das Serverzertifikat ordnungsgemäß installiert wurde. Klicken Sie auf **Zertifikate**, und doppelklicken Sie dann auf das neue Serverzertifikat. Die Registerkarte **Allgemein** sollte einen Hinweis enthalten, dass Sie einen privaten Schlüssel besitzen, der diesem Zertifikat entspricht. Auf der Registerkarte **Zertifizierungspfad** sehen Sie die hierarchische Beziehung zwischen dem Zertifikat und der Zertifizierungsstelle und den Hinweis **Dieses Zertifikat ist gültig**.

Aktualisieren von öffentlichen DNS

Erstellen Sie in den öffentlichen DNS-Servern einen neuen DNS-Hosteintrag. Benutzer stellen mit dem Namen der Website eine Verbindung her. Dieser Name muss dem gemeinsamen Namen bzw. dem FQDN (Fully Qualified Domain Name, vollqualifizierter Domänenname) des auf dem Computer mit ISA Server installierten Zertifikats entsprechen. Angenommen, ein Benutzer möchte **https://mail.contoso.com/exchange** aufrufen. In diesem Fall müssen die folgenden Bedingungen gegeben sein, damit er erfolgreich eine Verbindung herstellen kann:

- Der FQDN des auf dem Computer mit ISA Server installierten Serverzertifikats muss **mail.contoso.com** lauten.

  Wichtig:

  Contoso.com ist ein fiktiver Domänenname. Er wird hier lediglich zur Veranschaulichung verwendet und spielt in Ihrem speziellen Netzwerk keine Rolle. Der gemeinsame Name des Zertifikats muss mit dem FQDN übereinstimmen.
- Der Benutzer muss **mail.contoso.com** in eine IP-Adresse auflösen.

- Die IP-Adresse, in die **mail.contoso.com** aufgelöst wird, muss im externen Netzwerk des Computers mit ISA Server konfiguriert sein.

  Hinweis:

  Wenn Sie in ISA Server Enterprise Edition mit einem für den Netzwerklastenausgleich aktivierten Array arbeiten, ist die IP-Adresse möglicherweise eine für das Array konfigurierte virtuelle IP-Adresse. Weitere Informationen zum Netzwerklastenausgleich finden Sie in der Hilfe zu ISA Server.

Erstellen der Exchange ActiveSync-Webveröffentlichungsregel

Nachdem der Exchange-Clientzugriffsserver und der Computer mit ISA Server ordnungsgemäß konfiguriert und die richtigen Serverzertifikate installiert worden sind, können Sie mit den Verfahren zum Bereitstellen des Exchange-Clientzugriffsservers beginnen. Mit dem Assistent für neue Exchange-Veröffentlichungsregeln können Sie einen sicheren Zugriff auf Ihren Exchange-Front-End-Server ermöglichen.

Hinweis:

Sie können das Verfahren zum Erstellen einer ActiveSync-Webveröffentlichungsregel und eines Weblisteners vereinfachen, indem Sie das neue Update für ISA Server verwenden: http://go.microsoft.com/fwlink/?LinkID=87161&clcid=0x409.

Der Exchange-Clientzugriffsserver wird mit den folgenden Verfahren bereitgestellt:

- Erstellen eines Weblisteners
- Erstellen einer Veröffentlichungsregel für den Exchange-Webclientzugriff

Erstellen eines Weblisteners

Wenn Sie eine Webveröffentlichungsregel erstellen, müssen Sie einen Weblistener angeben. Die Eigenschaften des Weblisteners bestimmen Folgendes:

- IP-Adressen und Ports in den angegebenen Netzwerken, die der Computer mit ISA Server auf Webanforderungen abhört (HTTP oder HTTPS).
- Welche Serverzertifikate mit den IP-Adressen verwendet werden.
- Authentifizierungsmethode
- Anzahl der gleichzeitig möglichen Verbindungen
- Einstellungen für das einmalige Anmelden (Single Sign-On, SSO)

Sammeln Sie die folgenden Informationen, die beim Ausführen des Assistenten für neue Weblistener benötigt werden:

Eigenschaft	Wert
Weblistenername	Name: _____
Sicherheit der Clientverbindung Beachten Sie Folgendes: • Bei der Auswahl von **HTTP** werden die Informationen zwischen dem Computer mit ISA Server und dem Client als Klartext übertragen. • Bei der Auswahl von **HTTPS** muss auf dem Computer mit ISA Server ein Serverzertifikat installiert sein.	HTTPS oder HTTP (Zutreffendes markieren) **Wichtig:** Klartext kann zwar mit HTTP übertragen werden, es wird jedoch dringend empfohlen, die HTTPS-Option zum Konfigurieren des Weblisteners zu verwenden.

Weblistener-IP-Adressen	Netzwerk: _____ Optional Spezifische IP-Adresse: ___.___.___.___ **Hinweis:** Wenn diese spezifische IP-Adresse nicht die primäre IP-Adresse des Netzwerkadapters ist, muss zuerst eine sekundäre IP-Adresse auf dem Computer mit ISA Server konfiguriert werden. Anschließend kann der Weblistener erstellt werden.
Authentifizierungseinstellungen für das SSL-Zertifikat des Weblisteners **Hinweis:** Das ist nur erforderlich, wenn HTTPS für die Verbindungssicherheit des Clients ausgewählt wurde.	___Ein einziges Zertifikat für diesen Weblistener verwenden Zertifikat ist ausgestellt für: _____ ___Jeder IP-Adresse ein Zertifikat zuweisen (Diese Option ist nur verfügbar, wenn dem Weblistener eine spezifische IP-Adresse zugewiesen wurde. Das ist nur erforderlich, wenn der Listener mehrere IP-Adressen verwendet.) Zertifikat ist ausgestellt für: _____
Authentifizierung Bei der formularbasierten Authentifizierung sind Optionen verfügbar, um die Benutzer bei ISA Server zu authentifizieren. Wählen Sie die Authentifizierungsmethode, die Ihren Anforderungen am besten entspricht.	Weitere Informationen zur Authentifizierung finden Sie im Abschnitt zur Authentifizierung in ISA Server 2006 unter http://go.microsoft.com/fwlink/?LinkID=87068&clcid=0x409 (möglicherweise in englischer Sprache).
Einstellungen für einmaliges Anmelden (SSO). (Betrifft nur die formularbasierte Authentifizierung (FBA))	___Einmaliges Anmelden (SSO) aktivieren. SSO-Domäne: _____

Erstellen Sie anhand der Informationen in dem Arbeitsblatt einen Weblistener, und führen Sie dann das folgende Verfahren aus.

So erstellen Sie einen Weblistener

1. Klicken Sie in der Konsolenstruktur der ISA Server-Verwaltung auf **Firewallrichtlinie**.
   - Erweitern Sie in ISA Server 2006 Standard Edition **Microsoft Internet Security and Acceleration Server 2006**, erweitern Sie **Server_Name**, und klicken Sie dann auf **Firewallrichtlinie**.
   - Erweitern Sie in ISA Server 2006 Enterprise Edition **Microsoft Internet Security and Acceleration Server 2006**, erweitern Sie **Arrays**, erweitern Sie **Array_Name**, und klicken Sie dann auf **Firewallrichtlinie**.

2. Klicken Sie auf der Registerkarte **Toolbox** auf **Netzwerkobjekte**, klicken Sie auf **Neu**, und wählen Sie dann **Weblistener**. Erstellen Sie den Weblistener mithilfe des Assistenten wie in der folgenden Tabelle dargestellt.

Seite	Feld oder Eigenschaft	Einstellung
Willkommen	Weblistenername	Geben Sie einen Namen für den Weblistener ein. Beispiel: **Exchange FBA**.
Sicherheit der Clientverbindung	Wählen Sie die Art der Verbindungen aus, die dieser Weblistener mit Clients herstellen soll.	Wählen Sie **Sichere SSL-Verbindungen mit Clients erforderlich** aus.
Weblistener-IP-Adressen	In diesen Netzwerken auf eingehende Webanforderungen achten ISA Server komprimiert die Inhalte, die über diesen Weblistener an die Clients geschickt werden	Wählen Sie das externe Netzwerk aus. Das Kontrollkästchen sollte aktiviert sein (Standard). Klicken Sie auf **IP-Adressen auswählen**.
Auswahl der externen Netzwerklistener-IP	Anforderungen abhören auf Verfügbare IP-Adressen	Wählen Sie **Angegebenen IP-Adressen auf dem ISA Server-Computer im ausgewählten Netzwerk** aus. Wählen Sie die richtige IP-Adresse aus, und klicken Sie auf **Hinzufügen**. **Hinweis:** Wählen Sie bei ISA Server Enterprise Edition mit einem für den Netzwerklastenausgleich aktivierten Array eine virtuelle IP-Adresse aus.
Listener-SSL-Zertifikate	Wählen Sie ein Zertifikat für jede IP-Adresse aus, oder legen Sie ein einziges Zertifikat für diesen Weblistener fest.	Wählen Sie **Jeder IP-Adresse ein Zertifikat zuweisen** aus. Wählen Sie die gerade ausgewählte IP-Adresse aus, und klicken Sie auf **Zertifikat auswählen**.
Zertifikat auswählen	Wählen Sie aus der Liste verfügbarer Zertifikate ein Zertifikat aus.	Wählen Sie das Zertifikat aus, das Sie gerade auf dem Computer mit ISA Server installiert haben. Wählen Sie beispielsweise **mail.contoso.com** aus, und klicken Sie auf **Auswählen**. Das Zertifikat muss vor Ausführen des Assistenten installiert werden.

Seite	Feld oder Eigenschaft	Einstellung
Willkommen	Weblistenername	Geben Sie einen Namen für den Weblistener ein. Beispiel: **Exchange FBA**.
Authentifizierungs-einstellungen	Wählen Sie aus, wie Clients Anmeldeinformationen an ISA Server bereitstellen. Legen Sie fest, wie ISA Server die Client-Anmeldeinformationen überprüfen soll.	Wählen Sie **HTML-Formularauthentifizierung für formularbasierte Authentifizierung** aus, und wählen Sie die entsprechende Methode aus, mit der ISA Server die Client-Anmeldeinformationen überprüfen soll. Wählen Sie beispielsweise bei einer Installation im Arbeitsgruppenmodus **LDAP-Authentifizierung** aus. Wählen Sie **Windows (Active Directory)** aus, wenn der Computer mit ISA Server Mitglied einer Domäne ist.
Einstellungen für einmaliges Anmelden	SSO für Websites aktivieren, die mit diesem Weblistener veröffentlicht werden SSO-Domänenname	Behalten Sie zum Aktivieren von SSO die Standardeinstellungen bei. Wenn Sie SSO zwischen veröffentlichten Websites aktivieren möchten, wie z. B. **portal.contoso.com** und **mail.contoso.com**, geben Sie **.contoso.com** ein.
Fertigstellen des Assistenten	Fertigstellen des Assistenten	Überprüfen Sie die ausgewählten Einstellungen, und klicken Sie auf **Zurück**, um die Einstellungen zu ändern, und auf **Fertig stellen**, um den Assistenten abzuschließen.

Erstellen einer Veröffentlichungsregel für den Exchange-Webclientzugriff

Wenn Sie einen internen Exchange 2007-Clientzugriffsserver mit ISA Server 2006 bereitstellen, schützen Sie den Webserver vor direktem externen Zugriff, da der Benutzer nicht auf den Namen und die IP-Adresse des Servers zugreifen kann. Der Benutzer greift auf den Computer mit ISA Server zu, der dann die Anforderung an den internen Webserver weiterleitet. Dabei werden die Bedingungen der Webserver-Veröffentlichungsregel angewendet. Bei einer Veröffentlichungsregel für den Exchange-Webclientzugriff handelt es sich um eine Webveröffentlichungsregel, die geeignete Standardeinstellungen für den Exchange-Webclientzugriff enthält.

Sammeln Sie die folgenden Informationen, die Sie beim Ausführen des Assistenten für neue Exchange-Veröffentlichungsregeln benötigen:

Eigenschaft	Wert
Name der Exchange-Veröffentlichungsregel	Name: _____
Dienste **Hinweis:** Sie können mehrere Dienste mit einer einzigen Regel bereitstellen. Verwenden Sie dazu den gleichen Weblistener, der mit der formularbasierten Authentifizierung konfiguriert ist. In ISA Server 2006 wird die Standardauthentifizierung für Dienste verwendet, die keine formularbasierte Authentifizierung unterstützen.	Exchange -Version: _____ __Outlook Web Access __Outlook RPC over HTTP __Outlook Mobile Access _X_Exchange ActiveSync
Veröffentlichungstyp	__Eine einzelne Website veröffentlichen. oder __Serverfarm mit Webserver-Lastenausgleich veröffentlichen und Serverfarmname:_____
Sicherheit der Serververbindung	HTTPS oder HTTP (Zutreffendes markieren) Beachten Sie Folgendes: • Bei der Auswahl von **HTTP** werden die Informationen zwischen dem Computer mit ISA Server und dem Webserver als Klartext übertragen. • Bei der Auswahl von **HTTPS** muss auf dem Exchange-Front-End-Server ein Serverzertifikat installiert sein.

Interne Veröffentlichungsdetails	Interner Sitename (FQDN): _____ Geben Sie einen Computernamen oder eine IP-Adresse an, wenn der FQDN vom Computer mit ISA Server nicht aufgelöst werden kann: Computername oder IP-Adresse:_____ **Hinweis:** Muss mit dem gemeinsamen Namen des Upstreamzertifikats übereinstimmen.
Details des öffentlichen Namens	Anforderungen annehmen für: __Diesen Domänennamen:_____ oder __Jeden Domänennamen
Weblistener auswählen	Weblistener:_____
Benutzersatz	Führen Sie die Benutzersätze auf, die auf diese Regel zugreifen können: _____ _____ **Wichtig:** Wenn ISA Server nicht als Domänenmitglied konfiguriert ist und RADIUS verwendet wird, muss es sich dabei um nicht Windows-Benutzersätze handeln.

Im nächsten Verfahren erstellen Sie anhand der Informationen in diesem Arbeitsblatt eine Veröffentlichungsregel für den Exchange-Webclientzugriff.

Erstellen einer Veröffentlichungsregel für den Exchange-Webclientzugriff

So erstellen Sie eine Veröffentlichungsregel für den Exchange-Webclientzugriff

1. Klicken Sie in der Konsolenstruktur der ISA Server-Verwaltung auf **Firewallrichtlinie**.

- Erweitern Sie in ISA Server 2006 Standard Edition **Microsoft Internet Security and Acceleration Server 2006**, erweitern Sie **Server_Name**, und klicken Sie dann auf **Firewallrichtlinie**.
- Erweitern Sie in ISA Server 2006 Enterprise Edition **Microsoft Internet Security and Acceleration Server 2006**, erweitern Sie **Arrays**, erweitern Sie **Array_Name**, und klicken Sie dann auf **Firewallrichtlinie**.

2. Klicken Sie auf der Registerkarte **Aufgaben** auf **Exchange-Webclientzugriff veröffentlichen**. Erstellen Sie die Regel mithilfe des Assistenten, wie in der folgenden Tabelle dargestellt.

Verwenden Sie für einen einzelnen Webserver die folgende Tabelle **Assistent für neue Exchange-Veröffentlichungsregeln für eine einzelne Website**.

Assistent für neue Exchange-Veröffentlichungsregeln für eine einzelne Website

Seite	Feld oder Eigenschaft	Einstellung
Willkommen	Name der Exchange-Veröffentlichungs-regel	Geben Sie einen Namen für die Regel ein. Beispiel: **Exchange-Webclientveröffentlichung**.
Dienste auswählen	Exchange -Version Webclient-E-Mail-Dienste	Wählen Sie die richtige Version von Exchange aus. Beispiel: Exchange Server 2007 Wählen Sie die gewünschte Zugriffsmethode aus.
Veröffentlichungs-typ	Wählen Sie diese Option aus, wenn über die Regel eine einzelne Website oder ein externer Lastenausgleich, eine Webserverfarm oder mehrere Websites veröffentlicht werden sollen.	Wählen Sie **Einzelne Website oder Lastenausgleich veröffentlichen** aus.

Sicherheit der Serververbindung	Wählen Sie die Verbindungstypen aus, über die ISA Server eine Verbindung mit den veröffentlichten Webservern auf der Serverfarm aufnehmen soll.	Wählen Sie **SSL verwenden, um eine Verbindung zum veröffentlichten Webserver oder zur Serverfarm herzustellen** aus. **Hinweis:** Auf dem veröffentlichten Front-End-Server mit Exchange muss ein Serverzertifikat installiert sein. Außerdem muss das Zertifikat der Stammzertifizierungsstelle für die Zertifizierungsstelle, die das Serverzertifikat auf dem Front-End-Server mit Exchange ausgestellt hat, auf dem Computer mit ISA Server installiert sein.
Interne Veröffentlichungs-details	Interner Sitename	Geben Sie den internen FQDN des Exchange-Front-End-Servers ein. Beispiel: **exchfe.corp.contoso.com**. **Wichtig:** Der interne Sitename muss mit dem Namen des Serverzertifikats übereinstimmen, das auf dem internen Exchange-Front-End-Server installiert ist. **Hinweis:** Wenn der interne Sitename nicht richtig aufgelöst werden kann, können Sie **Name oder IP-Adresse eines Computers verwenden, um eine Verbindung zum veröffentlichten Server herzustellen** wählen. Geben Sie dann die erforderliche IP-Adresse oder den Namen ein, der vom Computer mit ISA Server aufgelöst werden kann.
Details des öffentlichen Namens	Anforderungen annehmen für Öffentlicher Name	Diesen Domänennamen (unten eingeben) Geben Sie den Domänennamen ein, für den ISA Server die Verbindung akzeptieren soll. Beispiel: **mail.contoso.com**.
Weblistener auswählen	Weblistener	Wählen Sie den zuvor erstellten Weblistener aus. Beispiel: **Exchange FBA**.
Authentifizierungsdelegierung	Legen Sie die Methode fest, mit der ISA Server sich beim veröffentlichten Webserver authentifizieren soll.	Wählen Sie die Standardauthentifizierung.

Benutzersätze	Diese Regel betrifft Anforderungen von folgenden Benutzersätzen	Wählen Sie den für den Zugriff auf diese Regel genehmigten Benutzersatz aus.
Fertigstellen des Assistenten für neue Exchange-Veröffentlichungsregeln	Fertigstellen des Assistenten für die neue Exchange-Veröffentlichung	Überprüfen Sie die ausgewählten Einstellungen, und klicken Sie auf **Zurück**, um die Einstellungen zu ändern, oder auf **Fertig stellen**, um den Assistenten abzuschließen.

Konfigurieren von ISA Server 2006 für die LDAP-Authentifizierung

Hinweis:
Dieser Schritt ist nur dann erforderlich, wenn der ISA Server 2006 kein Domänenmitglied ist.

Die LDAP-Authentifizierung (Lightweight Directory Access Protocol) ist mit der Active Directory-Authentifizierung vergleichbar, mit dem Unterschied, dass der Computer mit ISA Server kein Domänenmitglied sein muss. Zum Authentifizieren des Benutzers wird in ISA Server 2006 über das LDAP-Protokoll eine Verbindung mit einem konfigurierten LDAP-Server hergestellt. Auch Windows-Domänencontroller sind standardmäßig LDAP-Server. Weitere Konfigurationsänderungen sind nicht erforderlich. Die LDAP-Authentifizierung bietet folgende Vorteile:

- ISA Server 2006 Standard Edition- oder ISA Server 2006 Enterprise Edition-Arraymitglieder im Arbeitsgruppenmodus.
- Authentifizierung von Benutzern in einer Domäne, mit der keine vertrauenswürdige Beziehung besteht.
- In diesem Abschnitt wird Folgendes beschrieben:
- Erstellen eines LDAP-Serversatzes
- Erstellen eines LDAP-Benutzersatzes

Erstellen eines LDAP-Serversatzes

Führen Sie die folgenden Schritte aus, um einen LDAP-Serversatz zu erstellen:

- Wenn Sie ISA Server 2006 Standard Edition verwenden, führen Sie das folgende Verfahren auf dem Computer **isa01** aus.
- Wenn Sie ISA Server 2006 Enterprise Edition verwenden, führen Sie das folgende Verfahren auf dem Computer **storage01** aus.

So erstellen Sie einen LDAP-Serversatz

1. Klicken Sie in der Konsolenstruktur der ISA Server-Verwaltung auf **Allgemein**.
   - Erweitern Sie in ISA Server 2006 Standard Edition **Microsoft Internet Security and Acceleration Server 2006**, erweitern Sie **isa01**, erweitern Sie **Konfiguration**, und klicken Sie dann auf **Allgemein**.
   - Erweitern Sie in ISA Server 2006 Enterprise Edition **Microsoft Internet Security and Acceleration Server 2006**, erweitern Sie **Arrays**, erweitern Sie den Knoten für die Hauptarrays, erweitern Sie **Konfiguration**, und klicken Sie dann auf **Allgemein**.
2. Klicken Sie im Bereich **Details** auf **RADIUS- und LDAP-Server festlegen**.

3. Klicken Sie auf der Registerkarte **LDAP-Serversätze** auf **Hinzufügen**, um das Dialogfeld **LDAP-Serversatz hinzufügen** zu öffnen.
4. Geben Sie **CorpLDAP** in das Feld **LDAP-Serversatzname** ein.
5. Klicken Sie auf **Hinzufügen**, um jeweils den LDAP-Servernamen oder die IP-Adresse hinzuzufügen.
6. Geben Sie **dc01** in das Feld **Servername** ein, und klicken Sie auf **OK**.
7. Klicken Sie auf **OK**, um das Dialogfeld **LDAP-Serversatz hinzufügen** zu schließen.
8. Klicken Sie auf **Neu**, um das Dialogfeld **Neue LDAP-Serverzuordnung** zu schließen.
9. Geben Sie **corp*** in das Feld **Anmeldeausdruck** ein. Wählen Sie in **LDAP-Serversatz** den Eintrag **CorpLDAP** aus, und klicken Sie auf **OK**.
10. Klicken Sie auf **Schließen**, um das Fenster **Authentifizierungsserver** zu schließen.

Erstellen eines LDAP-Benutzersatzes

Um Benutzer durch LDAP zu authentifizieren, müssen Sie festlegen, welche Benutzer zu authentifizieren sind und wer die Benutzerauthentifizierung durchführt. Hierzu müssen Sie zunächst einen LDAP-Benutzersatz erstellen.
Führen Sie die folgenden Schritte aus, um einen LDAP-Benutzersatz zu erstellen:

- Wenn Sie ISA Server 2006 Standard Edition verwenden, führen Sie das folgende Verfahren auf dem Computer **isa01** aus.
- Wenn Sie ISA Server 2006 Enterprise Edition verwenden, führen Sie das folgende Verfahren auf dem Computer **storage01** aus.

So erstellen Sie einen LDAP-Benutzersatz
Klicken Sie in der Konsolenstruktur der ISA Server-Verwaltung auf **Firewallrichtlinie**.

Seite	Feld oder Eigenschaft	Einstellung
Willkommen	Benutzersatzname	Geben Sie **LDAPBenutzer** ein.
Benutzer	Wählen Sie Benutzer aus, die in diesem Benutzersatz enthalten sein sollen.	Klicken Sie auf **Hinzufügen**, und wählen Sie **LDAP**.
LDAP-Benutzer hinzufügen	LDAP-Serversatz Benutzername	Wählen Sie in der Dropdownliste den LDAP-Serversatz **CorpLDAP** aus. Wählen Sie **Alle Benutzer in diesem Namespace**. **Hinweis:** Sie können auch Benutzergruppen und bestimmte Benutzerkonten angeben, wenn nicht alle Benutzer zum LDAP-Benutzersatz gehören sollen.
Fertigstellen des Assistenten für neue Benutzersätze	Überprüfen Sie die Einstellungen.	Klicken Sie auf **Zurück**, um die Einstellungen zu ändern, oder auf **Fertig stellen**, um den Assistenten abzuschließen.

Klicken Sie anschließend im Detailbereich auf **Übernehmen**, um die Änderungen zu speichern und die Konfiguration zu aktualisieren.

Festlegen des Zeitlimits für Leerlaufsitzungen für Firewalls und Netzwerkgeräte auf 1800 Sekunden

In diesem Schritt ändern Sie das Zeitlimit für Leerlaufsitzungen für alle Firewalls, Proxyserver und Netzwerkgeräte, um die erforderliche Zeit für ein erfolgreiches Funktionieren der Direct Push-Technologie sicherzustellen.

Hinweis:

Das Standardzeitlimit für Leerlaufsitzungen ist in ISA Server 2006 auf die empfohlenen 1800 Sekunden (30 Minuten) festgelegt. Eine Änderung ist deshalb nicht notwendig.

Weitere Informationen zum Ändern des Zeitlimits für Leerlaufsitzungen finden Sie unter „Bewährte Methode: Konfigurieren der Firewall für eine optimale Direct Push-Leistung“ unter Bewährte Methoden für die Bereitstellung von Mobile Messaging und Grundlegendes zu Direct Push.

So überprüfen Sie das Zeitlimit für Leerlaufsitzungen der Firewall

1. Klicken Sie in der Konsolenstruktur der ISA Server-Verwaltung auf **Firewallrichtlinie**.
2. Klicken Sie auf der Registerkarte **Toolbox** auf **Netzwerkobjekte**.
3. Erweitern Sie in der Ordnerliste den Knoten **Weblisteners**, und zeigen Sie die Eigenschafen des entsprechenden Weblisteners an.
4. Klicken Sie auf die Registerkarte **Verbindungen**, und klicken Sie dann auf die Schaltfläche **Erweitert**.
5. Stellen Sie sicher, dass das **Verbindungszeitlimit** auf 1800 Sekunden (30 Minuten) festgelegt ist. Ändern Sie die Einstellung gegebenenfalls.
6. Klicken Sie zweimal auf **OK**, um eventuelle Änderungen zu übernehmen.
7. Klicken Sie auf **Übernehmen**, damit die Änderungen wirksam werden.

Testen der Exchange-Veröffentlichungsregel

In diesem Abschnitt testen Sie die neue Exchange-Veröffentlichungsregel, die Sie gerade erstellt haben.

Testen von Exchange ActiveSync

Konfigurieren Sie ein mobiles Gerät so, dass es mit Microsoft Exchange ActiveSync eine Verbindung mit Ihrem Exchange-Server herstellt. Stellen Sie dann fest, ob ISA Server und Exchange ActiveSync ordnungsgemäß funktionieren. Wenn Sie das mobile Gerät konfigurieren, werden Sie dazu aufgefordert, einen Servernamen einzugeben. Geben Sie dann den Namen des soeben bereitgestellten Exchange ActiveSync-Servers ein. Beispiel: **//mail.contoso.com/owa**.

Hinweis:

Sie können Exchange ActiveSync auch mit dem Internet Explorer testen. Öffnen Sie Internet Explorer, und geben Sie als Adresse folgende URL ein: **https://published_server_name/Microsoft-Server-Activesync**, wobei published_server_name der veröffentlichte Name des Outlook Web Access-Servers ist (der Name, mit dem ein Benutzer auf Outlook Web Access zugreift). Wenn die Fehlermeldung **Fehler 501/505 – Nicht implementiert oder nicht unterstützt** angezeigt wird, nachdem Sie sich authentifiziert haben, arbeiten ISA Server und Exchange ActiveSync ordnungsgemäß zusammen.

Schritt 5: Konfigurieren und Verwalten des Zugriffs über mobile Geräte auf den Exchange-Server

Mit der Installation von Microsoft Exchange Server 2007 werden Exchange ActiveSync-Features für alle mobilen Clientgeräte auf Organisationsebene aktiviert. Wenn Ihre Sicherheitskonfiguration die vertrauenswürdigen Zertifikate akzeptiert, die mit den mobilen Geräten geliefert werden, gibt es nicht mehr viel zu tun. Sie müssen die Benutzer, die mit Windows Mobile 6-basierten Geräten arbeiten, dann nur noch anweisen, sich mit der ActiveSync-Anwendung des Geräts anzumelden.

Hinweis:

In der Exchange-Verwaltungskonsole können Sie bei Bedarf eine zentrale Sicherheitsrichtlinie für alle Benutzer erstellen und konfigurieren. Folgen Sie dazu den Anweisungen unter „Konfigurieren der Sicherheitseinstellungen für mobile Geräte“ in diesem Kapitel.

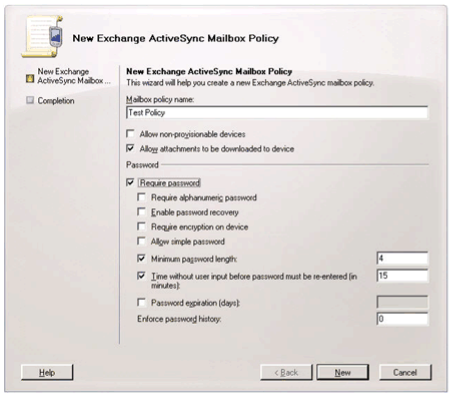
- Auf dem Exchange-Server können Sie folgende Verwaltungsfunktionen ausführen:
- Erstellen von Exchange ActiveSync-Postfachrichtlinien
- Konfigurieren der Sicherheitseinstellungen für mobile Geräte mit Postfachrichtlinien
- Anwenden einer Postfachrichtlinie auf einen Benutzer
- Ausführen einer Remotegerätzurücksetzung
- Deaktivieren von Exchange ActiveSync

Bei einer Standardinstallation von Exchange 2007 werden alle Features von Exchange ActiveSync aktiviert. Sie können die Einstellungen der Features über Exchange Server mit der Exchange-Verwaltungskonsole ändern, und Sie können Exchange ActiveSync-Features für einzelne Benutzer oder Gruppen mit Active Directory aktivieren oder deaktivieren.

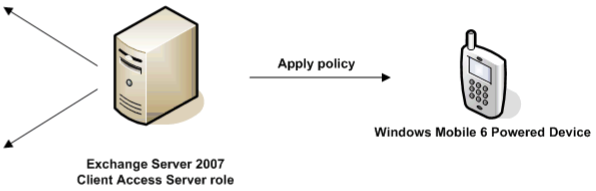
Erstellen von Exchange ActiveSync-Postfachrichtlinien

Vereinfachen Sie die Verwaltung der Exchange ActiveSync-Geräte, indem Sie Exchange ActiveSync-Postfachrichtlinien erstellen. Sie können diese Richtlinien für jeden Exchange ActiveSync-Benutzer anwenden und bestimmte Einstellungen für das Gerät eines Benutzers auf einfache Weise übernehmen. Eine Postfachrichtlinie enthält eine Reihe von Einstellungen für Microsoft Exchange ActiveSync. Diese Einstellungen betreffen das Kennwort, die Verschlüsselung und Anlagen. Wenn Sie die Client Access-Serverfunktion auf einen Computer mit Microsoft Exchange Server 2007 installieren, sind noch keine Postfachrichtlinien vorhanden. Sie können verschiedene Postfachrichtlinien erstellen und diesen Richtlinien Benutzer zuweisen.

Bereitstellen von Windows Mobile 6-basierten Geräten mit Microsoft Exchange Server 2007



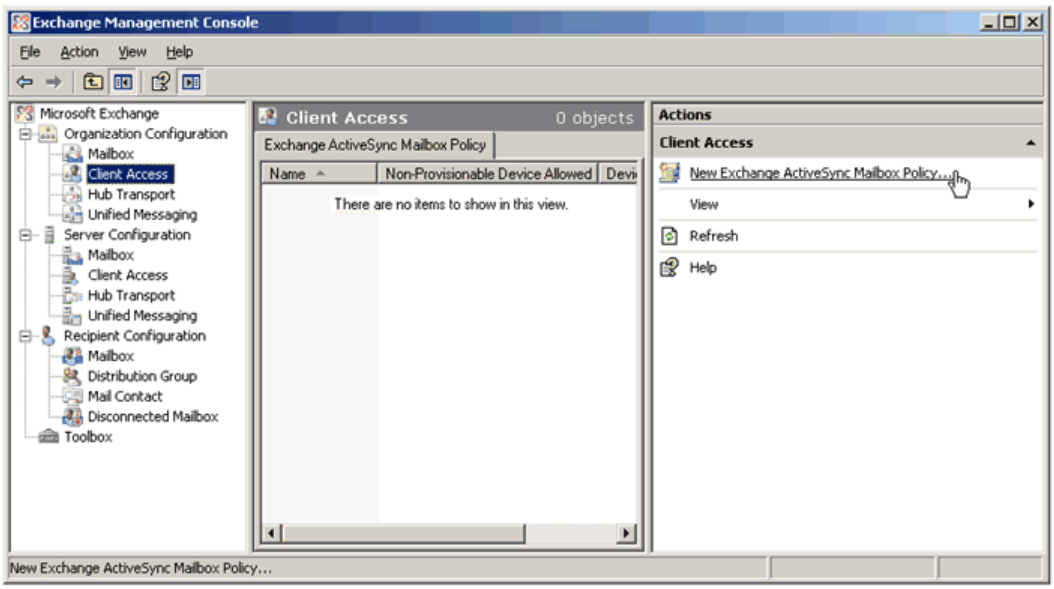
New Exchange ActiveSync Mailbox Policy configured through Exchange Management Console



Melden Sie sich an einem Computer, auf dem die Client Access-Serverfunktion installiert ist, mit einem Domänenkonto an, das über die Berechtigungen der Gruppe **Exchange-Empfängeradministrator** verfügt. Anschließend können Sie die folgenden Verfahren ausführen. Das Konto muss auch zur lokalen Gruppe **Administratoren** dieses Computers gehören.

Erstellen einer Exchange ActiveSync-Postfachrichtlinie mithilfe der Exchange-Verwaltungskonsole

1. Erweitern Sie in der Konsolenstruktur den Knoten **Organisationskonfiguration**, und klicken Sie dann auf **Clientzugriff**.



2. Klicken Sie im Aktionsbereich auf **Neue Exchange ActiveSync-Postfachrichtlinie**.
3. Geben Sie auf der Seite **Neue Exchange ActiveSync-Postfachrichtlinie** des Assistenten in das Feld **Name der Postfachrichtlinie** einen Namen ein.
4. Aktivieren Sie das Kontrollkästchen **Kennwort anfordern**, und aktivieren Sie eines oder mehrere der optionalen Kontrollkästchen.

5. Klicken Sie auf **Neu**.
6. Klicken Sie auf **Fertig stellen**, um den Assistenten **Neue Exchange ActiveSync-Postfachrichtlinie** zu schließen.

Konfigurieren der Sicherheitseinstellungen für mobile Geräte mit Postfachrichtlinien

Sie können Sicherheitsoptionen für Benutzer mobiler Geräte angeben, die eine Verbindung mit dem Exchange-Server herstellen. In der Exchange-Verwaltungskonsole können Sie Folgendes festlegen: die Länge und Sicherheit des Kennworts, die Dauer der Inaktivität und die Anzahl der fehlgeschlagenen Zugriffsversuche vor dem Zurücksetzen des mobilen Geräts.

Weitere Informationen zur Funktionsweise und zum Festlegen von Postfachrichtlinien finden Sie im Abschnitt zum Verwalten von Exchange ActiveSync mit Richtlinien unter http://go.microsoft.com/fwlink/?LinkID=87196&clcid=0x409 (möglicherweise in englischer Sprache).

Hinweis:

„Kennwort“ bezieht sich in diesem Kapitel auf das Kennwort, das ein Benutzer zum Entsperren seines mobilen Geräts eingibt. Dieses Kennwort hat nichts mit dem Benutzerkennwort für das Netzwerk zu tun.

Die folgende Tabelle zeigt, welche Art von Sicherheitsrichtlinien Sie festlegen können.

Exchange-Sicherheitsrichtlinien oder -Postfachrichtlinien	Exchange Server 2003 SP2	Exchange Server 2007
Kennwort für das Verwenden oder Konfigurieren des Geräts anfordern	X	X
Minimale Kennwortlänge festlegen	X	X
Alphanumerisches Kennwort anfordern	X	X
Angeben, nach wie vielen Minuten ohne Benutzereingabe das Gerät gesperrt wird	X	X
Geräte remote zurücksetzen	X	X
Speicherkarte remote löschen		X
Nicht bereitstellbare Geräte (vor Messaging and Security Feature Pack vertrieben) zulassen	X	X
Intervall für Geräteaktualisierung festlegen	X	X
Herunterladen von Anlagen zulassen oder verhindern		X
Maximale Anlagengröße festlegen		X
Verschlüsselung auf der austauschbaren Speicherkarte aktivieren		X
Datum für den Kennwortablauf festlegen		X
Kennwortwiederherstellung aktivieren		X
Muster in PIN (1111 oder 1234) des Geräts nicht zulassen		X

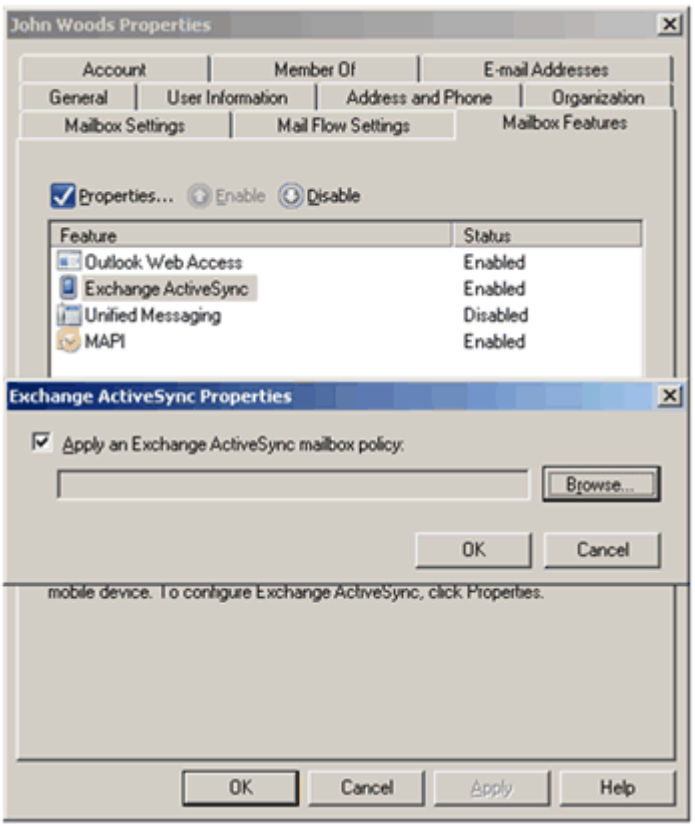
Anzahl der fehlgeschlagenen Kennworteingaben vor der Zurücksetzung des Geräts angeben	X	X
Anzahl der fehlgeschlagenen Kennworteingaben vor dem Löschen der Speicherkarte angeben		X
Zugriff auf Dateien in UNC-Freigaben (Universal Naming Convention) verhindern		X
Zugriff auf Dateien auf SharePoint Services-Websites zulassen oder verhindern		X

Anwenden einer Postfachrichtlinie auf einen Benutzer

Nachdem Sie eine Exchange ActiveSync-Postfachrichtlinie erstellt haben, können Sie Benutzer hinzufügen. Benutzer werden nicht standardmäßig einer Postfachrichtlinie zugewiesen. Ein Benutzer kann jeweils nur einer Postfachrichtlinie zugewiesen werden. Wenn Sie einer Exchange ActiveSync-Postfachrichtlinie einen Benutzer hinzufügen, der bereits einer anderen Exchange ActiveSync-Postfachrichtlinie zugewiesen ist, wird der Benutzer aus der ursprünglichen Exchange ActiveSync-Postfachrichtlinie entfernt und der neuen Exchange ActiveSync-Postfachrichtlinie hinzugefügt. Sie können einer Exchange ActiveSync-Postfachrichtlinie Benutzer einzeln oder in gefilterten Benutzergruppen hinzufügen.

So wenden Sie eine Postfachrichtlinie auf einen Benutzer an

1. Erweitern Sie in der Konsolenstruktur den Knoten **Empfängerkonfiguration**, und klicken Sie dann auf **Postfach**.
2. Klicken Sie im Arbeitsbereich mit der rechten Maustaste auf den Benutzer, den Sie einer Richtlinie zuweisen möchten, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie im Dialogfeld **Eigenschaften** auf **Postfachfeatures**.
4. Klicken Sie auf **ExchangeActiveSync**, und klicken Sie dann auf **Eigenschaften**.
5. Aktivieren Sie das Kontrollkästchen **Eine Exchange ActiveSync-Postfachrichtlinie anwenden**.



6. Klicken Sie auf **Durchsuchen**, um das Dialogfeld zum Auswählen der Postfachrichtlinie für das mobile Gerät anzuzeigen.
7. Wählen Sie eine verfügbare Richtlinie aus, und klicken Sie dann dreimal auf **OK**, um die Richtlinie anzuwenden.

Ausführen einer Remotegerätzurücksetzung

In diesem Abschnitt werden die Verfahren zum Ausführen einer Remotegerätzurücksetzung erläutert.

Remotegerätzurücksetzung im Vergleich zur lokalen Gerätzurücksetzung

Bei der lokalen Gerätzurücksetzung erfolgt die Zurücksetzung ohne Anforderung vom Server durch das Gerät selbst. Angenommen, die Organisation hat Exchange ActiveSync-Richtlinien implementiert, die z. B. eine maximale Anzahl von Kennwortversuchen zulassen. Wird dieses Maximum überschritten, führt das Gerät eine lokale Zurücksetzung aus. Das Ergebnis einer lokalen Gerätzurücksetzung ist dasselbe wie bei einer Remotegerätzurücksetzung. Das Gerät wird auf die Werkseinstellungen zurückgesetzt. Wenn ein Gerät eine Zurücksetzung ausführt, wird keine Bestätigung an den Exchange-Server gesendet.

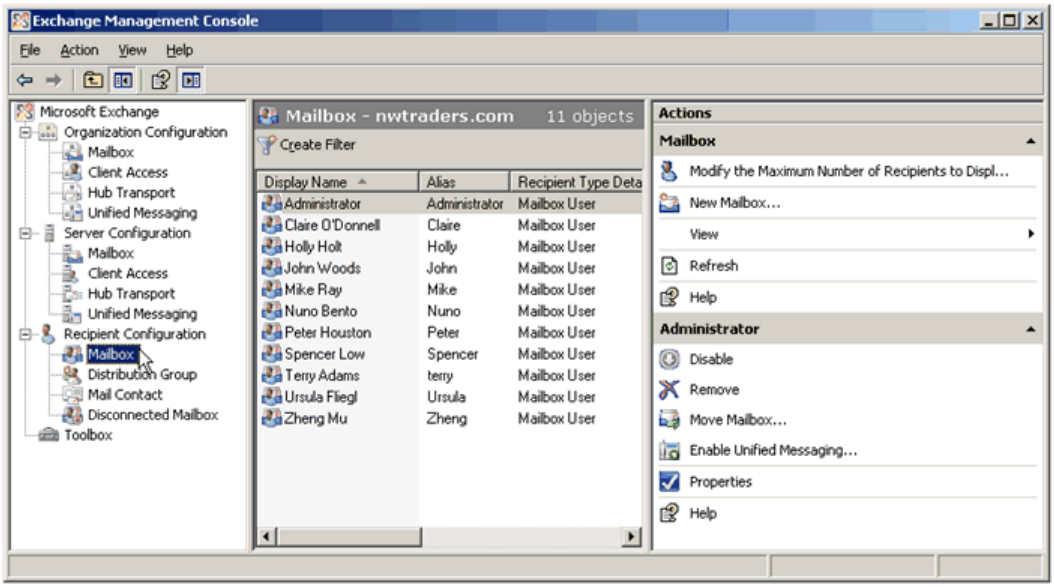
Hinweis:

Bei einer Remotegerätzurücksetzung wird das Gerät nicht nur auf die Werkseinstellungen zurückgesetzt, es werden auch alle Daten auf der Speicherkarte des Geräts gelöscht. Entfernen Sie zuerst die Speicherkarte, wenn Sie ein Gerät in Ihrem Besitz remote zurücksetzen und die Daten behalten möchten.

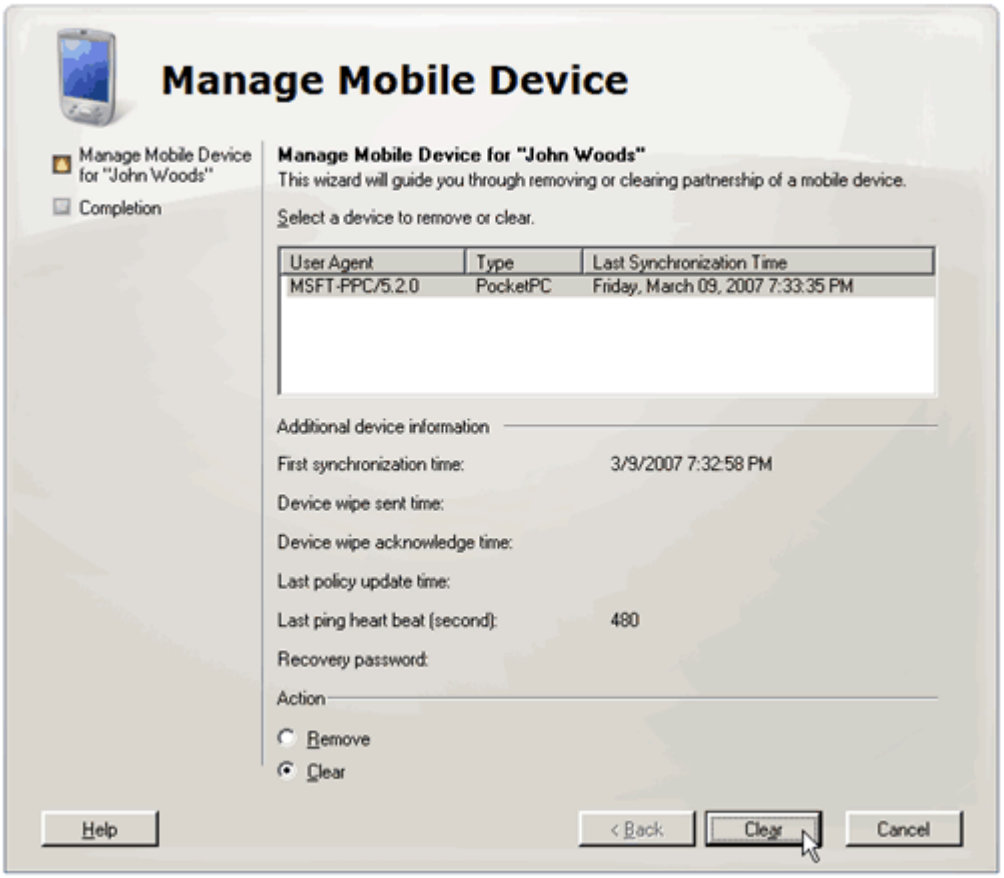
Bereitstellen von Windows Mobile 6-basierten Geräten mit Microsoft Exchange Server 2007

So führen Sie mit der Exchange-Verwaltungskonsole oder mit Outlook Web Access eine Remotegerätzurücksetzung aus

1. Öffnen Sie die Exchange-Verwaltungskonsole.
2. Wählen Sie unter **Empfängerkonfiguration** den Knoten **Postfach** aus.



3. Wählen Sie im Fenster **Postfach** den Benutzer aus.
4. Klicken Sie im Aktionsbereich auf **Mobiles Gerät verwalten**. Oder klicken Sie mit der rechten Maustaste auf das Postfach des Benutzers, und klicken Sie dann auf **Mobiles Gerät verwalten**.
5. Wählen Sie das mobile Gerät aus, das Sie zurücksetzen möchten.
6. Klicken Sie im Abschnitt **Aktion** auf die Schaltfläche **Löschen**.



7. Klicken Sie auf **Löschen** unten im Fenster, um den Vorgang abzuschließen.

So führen Sie mit Outlook Web Access eine Remotegerätzurücksetzung aus:

1. Öffnen Sie Outlook Web Access.
2. Melden Sie sich beim Postfach des Gerätebesitzers an.
3. Klicken Sie auf **Optionen**.
4. Wählen Sie im Navigationsbereich **Mobile Geräte** aus.
5. Wählen Sie die ID des Geräts aus, das Sie zurücksetzen und aus der Liste entfernen möchten.
6. Klicken Sie auf **Alle Daten auf dem Gerät löschen**.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Gerät aus Liste entfernen**.

Deaktivieren von Exchange ActiveSync

In diesem Abschnitt wird beschrieben, wie Microsoft Exchange ActiveSync deaktiviert wird. Wenn Sie Exchange ActiveSync auf einem Computer deaktivieren, auf dem Microsoft Exchange Server 2007 mit der installierten Client Access-Serverfunktion ausgeführt wird, deaktivieren Sie den von Exchange ActiveSync verwendeten Anwendungspool. Ein Anwendungspool ist eine Gruppe von Prozessen, die von Internetinformationsdienste (IIS) verwendet werden, um eine Aufgabe auszuführen.

Hinweis:

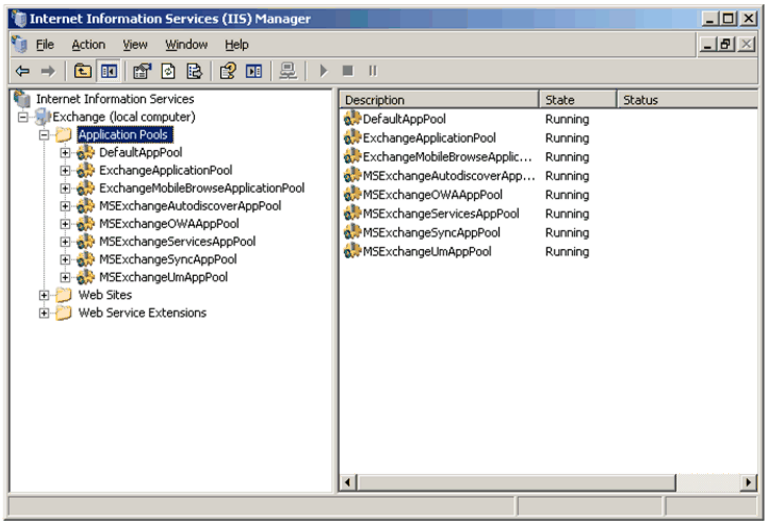
Dieser Leitfaden behandelt in erster Linie das Implementieren eines Mobile Messaging-Systems, in dem Exchange ActiveSync aktiviert ist. Bei der Wartung der Netzwerkinfrastruktur oder des Mobile Messaging-Systems und zu Testzwecken kann das Deaktivieren dieser Funktionalität jedoch gelegentlich erforderlich sein.

Melden Sie sich an einem Computer, auf dem die Client Access-Serverfunktion installiert ist, mit einem Domänenkonto an, das über die Berechtigungen der Gruppe **Exchange-Organisationsadministratoren** verfügt. Anschließend können Sie die folgenden Verfahren ausführen. Das Konto muss auch zur lokalen Gruppe **Administratoren** dieses Computers gehören.
Überprüfen Sie außerdem Folgendes, bevor Sie diese Verfahren ausführen:

- Die Komponente Microsoft ASP.NET von Microsoft Internetinformationsdienste (IIS) ist installiert.
- Der Status der ASP.NET-Webdiensterweiterung ist auf **Zugelassen** festgelegt. Sie können den Status der ASP.NET-Webdiensterweiterung in der IIS-Verwaltung überprüfen. Erweitern Sie dazu den Servernamen, und klicken Sie auf **Webdiensterweiterungen**. Falls die ASP.NET-Webdiensterweiterung nicht auf **Zugelassen** festgelegt ist, klicken Sie mit der rechten Maustaste auf die Webdiensterweiterung, und ändern Sie den Status.

So deaktivieren Sie Exchange 2007 ActiveSync mithilfe der IIS-Verwaltung

1. Klicken Sie auf **Start**, klicken Sie auf **Verwaltung**, und klicken Sie dann auf **Internetinformationsdienste-Manager**.
2. Doppelklicken Sie auf den Servernamen, um die Struktur zu erweitern. Doppelklicken Sie dann auf **Anwendungspools**, um den Ordner zu erweitern.



3. Klicken Sie mit der rechten Maustaste auf **MSExchangeSyncAppPool**, und klicken Sie dann auf **Beenden**, um Exchange ActiveSync zu deaktivieren.

Hinweis:
Ist der Befehl **Beenden** nicht verfügbar, dann ist Exchange ActiveSync auf diesem Server bereits deaktiviert.

Weitere Informationen zum Aktivieren von Exchange ActiveSync finden Sie unter Verwalten von Exchange ActiveSync (möglicherweise in englischer Sprache).

Schritt 6: Zertifikatregistrierung und Geräteprovisioning

In diesem Abschnitt werden digitale Zertifikate erläutert. Sie erfahren, wie Sie Ihre mobilen Geräte mit digitalen Zertifikaten identifizieren und einen sicheren Authentifizierungspfad für den Zugriff auf das Unternehmensnetzwerk bereitstellen. Außerdem wird das Geräteprovisioning beschrieben, das bei der Verwaltung von Geräten in Unternehmen hilfreich sein kann.

Zertifikate auf Windows Mobile-basierten Geräten

Digitale Zertifikate spielen eine wichtige Rolle bei der Authentifizierung im Netzwerk und beim Sichern von Geräten. Zertifikate sind elektronische Anmeldeinformationen, die die Identität des Zertifikatbesitzers oder des Geräts an ein aus einem öffentlichen und einem privaten Schlüssel bestehendes Paar elektronischer Schlüssel binden, das zum Verschlüsseln und digitalen Signieren von Informationen dient. Mithilfe signierter digitaler Zertifikate kann sichergestellt werden, dass die Schlüssel tatsächlich zu der angegebenen Anwendung, dem Gerät, der Organisation oder der Person gehören und vertrauenswürdig sind.
Digitale Zertifikate werden auf Windows Mobile-basierten Geräten in zwei entscheidenden Vorgängen verwendet:

- Bei der Authentifizierung. Dabei dienen sie dazu, vertrauenswürdige Anmeldeinformationen zum Herstellen einer Verbindung mit dem E-Mail-Server oder Netzwerk eines Unternehmens bereitzustellen oder die Identität eines Remoteservers zu überprüfen.
- Beim Signieren von Code. Dabei kann ermittelt werden, ob eine Anwendung auf dem Gerät ausgeführt werden darf und wenn ja, mit welchen Berechtigungen (höher oder normal) sie ausgeführt wird.

Für eine Authentifizierung in einem Netzwerk beispielsweise muss das mobile Gerät ein Zertifikat aus seinem Stammspeicher vorlegen, das vom Server erkannt und akzeptiert werden muss, bevor eine SSL-Verbindung mit dem Netzwerkserver hergestellt werden kann.
Außerdem muss eine Anwendung, damit sie auf einem Gerät installiert und ausgeführt werden kann, ein digitales Zertifikat aufweisen. Das Zertifikat muss belegen, dass die Anwendung von einer vertrauenswürdigen Quelle akzeptiert und signiert wurde.

Zertifikate auf Windows Mobile-basierten Geräten

Windows Mobile-basierte Geräte sind standardmäßig bereits mit verschiedenen Zertifikaten ausgestattet:

- Vertrauenswürdige Stammzertifikate von führenden Zertifikatherstellen, die zur Authentifizierung verwendet werden können.
- Mobile2Market und andere vertrauenswürdige Zertifikate, mit denen Anwendungen ausgewiesen werden, die für die Verwendung auf Windows Mobile-basierten Geräten signiert sind.
- Weitere Zertifikate, die vom OEM oder Mobilfunkbetreiber hinzugefügt werden.

Die folgende Tabelle enthält die mit Windows Mobile 6-basierten Geräten gelieferten Zertifikate (zum Zeitpunkt der Drucklegung).

Anbieter	Zertifikatname
Comodo	AAA Certificate Services
Comodo	AddTrust External CA Root
Cybertrust	Baltimore CyberTrust Root

Cybertrust	GlobalSign Root CA
Cybertrust	GTE CyberTrust Global Root
Verisign	Class 2 Public Primary Certification Authority
Verisign	Thawte Premium Server CA
Verisign	Thawte Server CA
Verisign	Secure Server Certification Authority
Verisign	Class 3 Public Primary Certification Authority
Entrust	Entrust.net Certification Authority (2048)
Entrust	Entrust.net Secure Server Certification Authority
Geotrust	Equifax Secure Certification Authority
Geotrust	GeoTrust Global CA
Godaddy	Go Daddy Class 2 Certification Authority
Godaddy	http://www.valicert.com/
Godaddy	Starfield Class 2 Certification Authority

Zertifikatspeicher

Die Zertifikate eines Windows Mobile-basierten Geräts befinden sich im Zertifikatspeicher in der Registrierung. In der Windows Mobile 6-Software enthält der Zertifikatspeicher getrennte Benutzerspeicher für Stammzertifikate und Zertifizierungsstellen. Benutzer mit weniger umfassenden Berechtigungen erhalten dadurch die Möglichkeit, vertrauenswürdige digitale Zertifikate hinzuzufügen oder zu registrieren. Der Stammzertifikat- und der Zertifizierungsstellenspeicher des Systems können nur mit den Berechtigungen der Rollen **Manager** oder **Enterprise** geändert werden.

Hinweis:

Auf Windows Mobile 5.0-basierten Geräten sind die Stammzertifikat- und Zertifizierungsstellenspeicher der digitalen Zertifikate generell gesperrt, außer für Berechtigungen der Rolle **Manager**.

Die folgende Tabelle zeigt die Verwendung und Berechtigungen der Zertifikatspeicher eines Windows Mobile 6-basierten Geräts.

Zertifikatspeicher	Physikalischer Speicher	Beschreibung
Privileged Execution Trust Authorities	HKLM	Enthält vertrauenswürdige Zertifikate. Anwendungen, die mit einem Zertifikat aus diesem Speicher signiert sind, werden mit einer höheren Vertrauensstufe ausgeführt (vertrauenswürdig).
Unprivileged Execution Trust Authorities	HKLM	Enthält normale Zertifikate. Auf einem einstufigen Gerät wird eine Anwendung, die mit einem Zertifikat aus diesem Speicher signiert ist, mit einer höheren Vertrauensstufe ausgeführt (privilegiert). Auf einem zweistufigen Gerät werden Anwendungen, die mit einem Zertifikat aus diesem Speicher signiert sind, mit einer normalen Vertrauensstufe ausgeführt (normal).
SPC	HKLM	Enthält Softwareherausgeberzertifikate (Software Publishing Certificates, SPC) zum Signieren von CAB- oder CPF-Dateien und zum Zuweisen der richtigen Rollenberechtigungen für die Dateiinstallation.
Root (system)	HKLM	Enthält die Stammzertifikate, d. h. Zertifikate, die von Microsoft, dem OEM oder dem Mobilfunkbetreiber signiert sind. Diese Zertifikate werden zur SSL-Serverauthentifizierung verwendet. Diese Zertifikate können nur mit Berechtigungen der Rolle **Manager** geändert werden. Benutzer mit der Rolle **Manager** können diesem Speicher Zertifikate hinzufügen. Der OMA DM-Transportclient überprüft diesen Speicher beim Herstellen einer SSL-Verbindung auf Stammzertifikate.
Root (user)	HKCU	Enthält Stamm- oder selbstsignierte Zertifikate, die von Benutzern mit der Rolle **Authentifizierter Benutzer** installiert werden können.
CA (system)	HKLM	Enthält Zertifikate und Informationen von Zwischenzertifizierungsstellen. Mit diesen Stellen werden Zertifikatketten gebildet. In Windows Mobile 5.0 können Benutzer mit der Rolle **Manager** diesem Speicher Zertifikate hinzufügen. Der OMA DM-Transportclient überprüft diesen Speicher beim Herstellen einer SSL-Verbindung auf Zwischenzertifikate. Diesem Speicher werden von Microsoft, dem OEM oder dem Mobilfunkbetreiber Zertifikate hinzugefügt.

CA (user)	HKCU	Enthält Zertifikate, einschließlich derer von Zwischenzertifizierungsstellen, die vom Gerätenutzer mit der Rolle **Authentifizierter Benutzer** installiert werden können. Mit diesen Stellen werden Zertifikatketten gebildet.
MY	HKCU	Enthält Endbenutzern gehörende persönliche Zertifikate, die für die Zertifikatauthentifizierung oder S/MIME verwendet werden.

Zertifikatketten

Eine Zertifikatkette besteht aus allen Zertifikaten, die für die Zertifizierung des Objekts benötigt werden, das mit dem Endzertifikat identifiziert wird. In der Praxis gehören dazu das Endzertifikat, die Zertifikate der Zwischenzertifizierungsstellen und das Zertifikat einer Stammzertifizierungsstelle, die für alle Beteiligten der Kette als vertrauenswürdig gilt. Jede Zwischenzertifizierungsstelle in der Kette besitzt ein Zertifikat, das von der übergeordneten Stelle in der Vertrauenshierarchie ausgestellt wurde. Die Stammzertifizierungsstelle stellt sich ein eigenes Zertifikat aus.

Beim Importieren des Zertifikats für einen Client kann die Zertifikatkette in die Datei eingeschlossen werden. Dadurch können die mit dem Endzertifikat verbundenen Zwischenzertifikate und das Stammzertifikat vom Gerät authentifiziert werden. Alle Zertifikate in der Kette werden den entsprechenden Zertifikatspeichern des Geräts hinzugefügt, um eine Überprüfung der Vertrauensstellung zu ermöglichen.

Standardauthentifizierung

Exchange ActiveSync verwendet SSL, um die Verbindung zwischen dem Windows Mobile-basierten Gerät und dem Exchange-Front-End oder -Clientzugriffsserver zu sichern. Das Clientgerät übermittelt die Anmeldeinformationen des Domänenbenutzers anhand der SSL-Standardauthentifizierung. Dabei wird der Client beim Server authentifiziert. Das Gerät muss über das Stammzertifikat des Exchange-Front-End-Servers oder -Clientzugriffsservers verfügen, damit eine sichere Verbindung hergestellt werden kann.

Windows Mobile-basierte Geräte sind mit einer Reihe von vertrauenswürdigen Stamm- und Zwischenzertifikaten ausgestattet. Wenn Sie eines dieser vertrauenswürdigen Zertifikate zum Schutz Ihres Exchange-Servers verwenden, können Benutzer dieser Geräte auf Ihr Unternehmensnetzwerk zugreifen, indem sie ihre Domäne, ihren Namen und ihr Kennwort eingeben.

Hinweis:

Platzhalterzertifikate, d. h. Zertifikate, die nicht von einem Microsoft-Zertifizierungsstellenserver stammen, können mit Windows Mobile 6-basierten Geräten verwendet werden.

Zertifikatbasierte Authentifizierung

Windows Mobile 5.0-basierte Geräte mit dem Messaging and Security Feature Pack oder neuere Geräte können die TLS-Clientauthentifizierung (Transport Layer Security) anstelle der SSL-Standardauthentifizierung verwenden. Die zertifikatbasierte Authentifizierung bietet gewisse Sicherheitsvorteile gegenüber der einstufigen kennwortbasierten Authentifizierung. Dieser Vorteil basiert auf zwei Faktoren. Erstens wird die Sicherheit des Schlüssels vom Administrator bestimmt und kann sehr hoch sein. Windows Mobile und Windows Server unterstützen zusammen bis zu 2.048-Bit-Schlüssel. Zweitens verringert das Voraussetzen einer zertifikatbasierten Authentifizierung das Risiko erheblich, dass die Anmeldeinformationen des Benutzers in falsche Hände gelangen.

Wenn ein Benutzer sein Kennwort weitergibt, verhindert der Authentifizierungsprozess, dass ein Angreifer verwendbare Anmeldeinformationen an sich bringen kann. Die Anmeldeinformationen werden hashcodiert und durch eine SSL-Verschlüsselung bei der Übermittlung geschützt.

Damit eine zertifikatbasierte Authentifizierung mit Windows Mobile für das mobile Gerät verwendet werden kann, benötigt das Gerät das Stammzertifikat für den Exchange Server-Front-End- oder den Clientzugriffsserver, mit dem es die Verbindung herstellt. Das mobile Gerät muss außerdem über ein eigenes Clientbenutzerzertifikat mit dem zugehörigen privaten Schlüssel verfügen. Die Registrierung des Benutzerzertifikats kann nur dann erfolgen, wenn das Gerät mit einem Desktop verbunden ist, der zur selben Domäne gehört wie die Registrierungswebsite.

Verwalten von Gerätezertifikaten

Digitale Zertifikate sind ein leistungsstarkes Tool, um Geräte und Benutzer für die Authentifizierung mit einer Identität zu versehen. Allerdings kann das Verteilen und Erneuern von digitalen Zertifikaten auf Hunderten oder Tausenden mobiler Geräte in einem Unternehmen eine mühsame Aufgabe werden. Mit der Windows Mobile 6-Software und Desktop ActiveSync ist die Verwaltung von Gerätezertifikaten nun viel einfacher geworden. Die Zertifikatregistrierungstools ermöglichen es dem Administrator, durch das Verwalten von Gerätezertifikaten eine sicherere Umgebung zu schaffen.

Sie können die Windows Mobile 6-Software und ActiveSync-Zertifikatregistrierungstools für die folgenden unternehmensweiten Aktivitäten verwenden:

- Bereitstellen einer Exchange ActiveSync- oder zertifikatbasierten SSL/TLS-Authentifizierung im gesamten Unternehmen
- Erneuern vorhandener Zertifikate
- Verteilen von 082.1x-Zertifikaten für drahtlose Netzwerke
- Bereitstellen von Zertifikaten für digitale S/MIME-Signaturen

Das Verfahren zum Hinzufügen von Zertifikaten unterscheidet sich bei Windows Mobile 5.0- und Windows Mobile 6-basierten Geräten.

Hinzufügen von Zertifikaten zu Windows Mobile 5.0-basierten Geräten

Um einem Windows Mobile 5.0-basierten Gerät ein Zertifikat hinzuzufügen, benötigen Sie die Berechtigungen der Rolle **Manager** für das Gerät, oder Sie müssen den vertrauenswürdigen Code auf dem Gerät ausführen können. Sie können beim OEM oder Mobilfunkbetreiber auch ein signiertes Zertifikatinstallationstool anfordern, z. B. **SPADDCERT.exe**.

Wenn Sie Stammzertifikate für die zertifikatbasierte Authentifizierung installieren möchten, können Sie das Tool für die Bereitstellung einer zertifikatbasierten Exchange ActiveSync-Authentifizierung verwenden. Das Tool kann auf der Microsoft Download Center-Website heruntergeladen werden: http://go.microsoft.com/fwlink/?LinkId=54738.

Weitere Informationen finden Sie im Knowledge Base-Artikel zum Installieren von Stammzertifikaten auf einem Windows Mobile-Gerät auf der folgenden Website von Microsoft: http://go.microsoft.com/fwlink/?LinkID=89647&clcid=0x409 (möglicherweise in englischer Sprache).

Hinzufügen von Zertifikaten zu Windows Mobile 6-basierten Geräten

Sie können für Windows Mobile 6-basierte Geräte eine CAB-Datei mit einem für Ihre Organisation geeignetem Zertifikat erstellen. Die Rolle **Benutzer** ermöglicht den Benutzern, diese CAB-Datei zu installieren, um das Zertifikat dem Stamm- und dem Zertifizierungsstellenspeicher im HKCU-Speicher des Geräts hinzuzufügen.

Sie können auch die Registrierfunktion der Exchange ActiveSync-Desktopsoftware verwenden, um das verschlüsselte Zertifikat und Schlüsselpaar für die zertifikatbasierte Authentifizierung oder für die 802.1x-Funkverbindung zu verteilen.

Das Zertifikatinstallationsprogramm auf Windows Mobile 6-basierten Geräten installiert in den folgenden Formaten erhaltene Zertifikate:

- PFX/.P12 – Public-Key Cryptography Standards #12 (PKCS #12) – Dateien, die persönliche Zertifikate mit privaten Schlüsseln enthalten, und Zertifikate, die in den Zwischen- und Stammzertifikatspeichern installiert werden.
- CER – Base64-codierte oder DER-codierte X.509-Zertifikate, die in den Zwischen- und Stammzertifikatspeichern installiert werden.
- P7B - Public-Key Cryptography Standards #7 (PKCS #7) – Dateien, mit denen mehrere Zertifikate in beliebige Zertifikatspeicher des Geräts installiert werden.

Es gibt folgende Möglichkeiten, die Dateien auf das Gerät zu übertragen: Desktop ActiveSync, austauschbare Speicherkarten, E-Mail-Anlagen oder Mobile Internet Explorer-Dateidownload. Windows Mobile 6 Professional-basierte Geräte ermöglichen auch einen Download aus einer Dateifreigabe. Beim Öffnen der Datei im Datei-Explorer wird die Datei vom Zertifikatinstallationsprogramm automatisch verarbeitet und installiert.

Hinweis:

Benutzer mit den Berechtigungen der Rolle **Benutzer** können ein Zertifikat auf einem Windows Mobile 6-basierten Gerät installieren, indem Sie die CAB- oder CER-Datei auf das Gerät kopieren und ausführen. Zur Registrierung eines Zertifikats über eine Zertifizierungsstelle sollten die Benutzer der Geräte jedoch Desktop ActiveSync verwenden.

Verwenden der Desktop-Registrierung

Desktop ActiveSync ermöglicht Benutzern von Windows Mobile-basierten Geräten mit einem Cradle die Zertifikatregistrierung über den Unternehmensserver auszuführen. Die Benutzer stellen über das übliche Desktopanmeldeverfahren des Unternehmens eine Verbindung mit dem Netzerwerk her, d. h. über Kennwort, Smartcard oder eine sonstige Art der Benutzeridentifikation. Die beiden Ebenen der Authentifizierung steuern die Zertifikatregistrierung und vereinfachen das Verteilen von Zertifikaten.

Mithilfe der Desktop-Zertifikatregistrierung können Zertifikate auf mobilen Geräten angefordert oder erneuert werden. Sie können auch den Certificate Enroller Configuration Service Provider (Konfigurationsdienstanbieter der Zertifikatregistrierung) verwenden, um Zertifikatdateien zu definieren und die XML-Provisioningdatei zu erstellen, die per Push auf mobile Geräte verteilt werden kann.

Der Systemadministrator sollte die Desktop-Zertifikatregistrierung folgendermaßen vorbereiten:

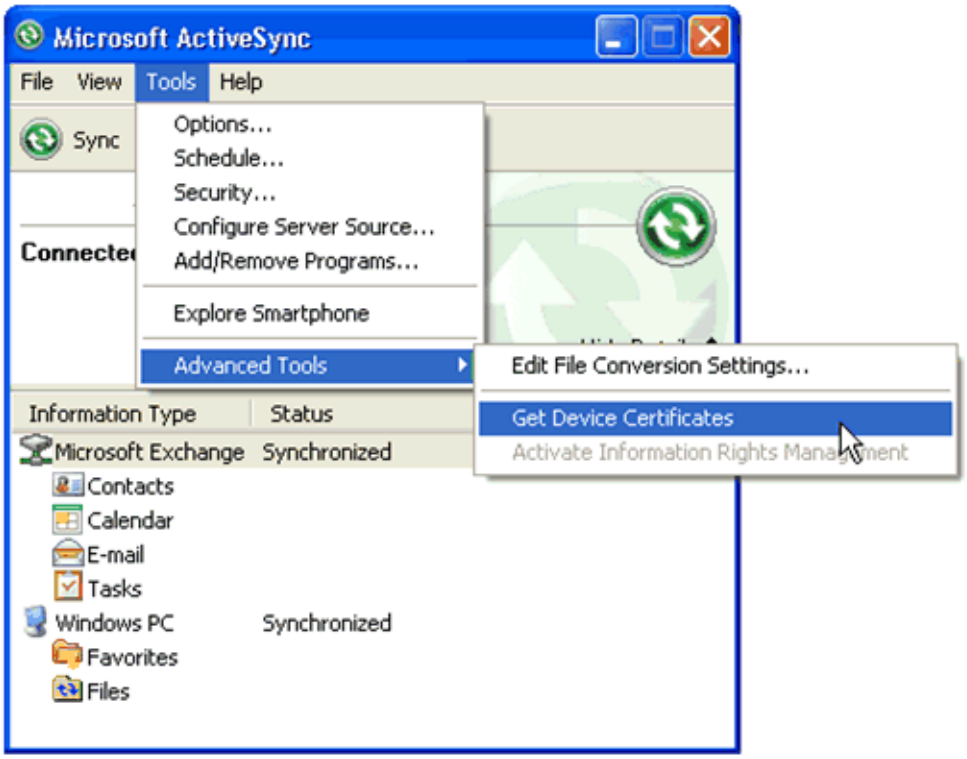
- Einrichten eines Windows 2000-, Windows 2003-Zertifikatservers oder höher, oder den Zugriff darauf sicherstellen.
- Erstellen des Zertifikattyps oder Verwenden eines vorhandenen Zertifikats, das in Active Directory veröffentlicht ist.
- Informieren der Benutzer über den Speicherort des Zertifikats im Unternehmensnetzwerk.
- Bereitstellen von Anweisungen für die Benutzer zur Verwendung des ActiveSync-Features **Get Device Certificate** (Gerätezertifikat abrufen) auf dem Desktop-PC.

Bereitstellen von Windows Mobile 6-basierten Geräten mit Microsoft Exchange Server 2007

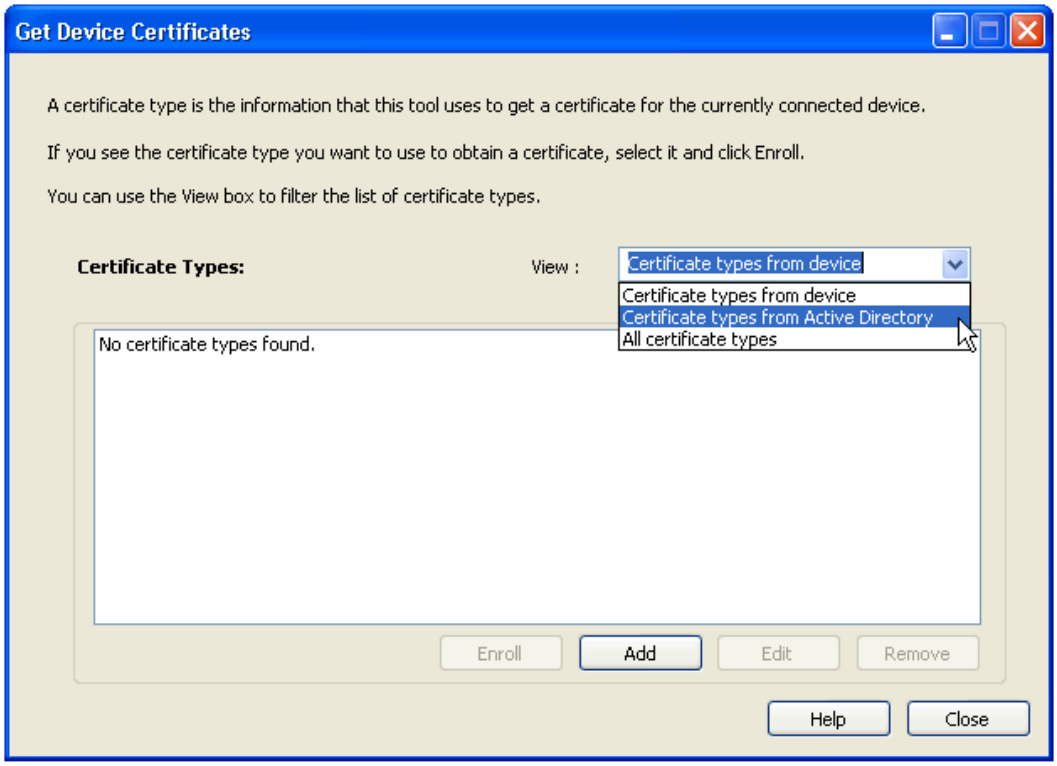
Nachdem Sie das Zertifikat in Active Directory veröffentlicht haben und die Gerätebenutzer zur Zertifikatregistrierung angeleitet haben, führen die Benutzer das folgende Verfahren aus:

So führen Sie eine Zertifikatregistrierung bei einem Windows Mobile 6-basierten Gerät aus

1. Synchronisieren Sie das Windows Mobile-basierte Gerät mithilfe von ActiveSync mit einem Desktopcomputer, und melden Sie sich am Unternehmensnetzwerk in derselben Domäne an, in der sich der Zertifikatregistrierungsserver befindet.



2. Wählen Sie unter **Advanced Tools** (Erweiterte Tools) die Option **Get Device Certificates** (Gerätezertifikat abrufen). Wählen Sie im Dialogfeld **Get Device Certificates** (Gerätezertifikat abrufen) in der Dropdownliste **View** (Ansicht) den Eintrag **Certificate types from Active Directory** (Zertifikattypen aus Active Directory) aus, wählen Sie das gewünschte Zertifikat in der Liste aus, und klicken Sie auf **Enroll** (Registrieren).


Get Device Certificates
A certificate type is the information that this tool uses to get a certificate for the currently connected device.
If you see the certificate type you want to use to obtain a certificate, select it and click Enroll.
You can use the View box to filter the list of certificate types.
Certificate Types:
View :
Certificate types from device
Certificate types from device
Certificate types from Active Directory
All certificate types
No certificate types found.
Enroll
Add
Edit
Remove
Help
Close

3. Klicken Sie in **Get Device Certificate** (Gerätezertifikat abrufen) auf **Yes** (Ja), um fortzufahren.
4. Damit die Zertifikatanforderung auf dem Windows Mobile 6-basierten Gerät genehmigt werden kann, wird ein Gerätebildschirm angezeigt, in dem Sie die Installation bestätigen müssen. Klicken Sie auf dem Gerät auf **Continue** (Weiter).
5. Möglicherweise werden Sie auf dem Gerät ein zweites Mal gefragt, ob das Zertifikat installiert oder die Anforderung blockiert werden soll. Wählen Sie **Install** (Installieren).
6. Der Desktopcomputer verarbeitet die Registrierung. Währenddessen wird vom Gerät ein Schlüsselpaar (privater/öffentlicher Schlüssel) generiert und die Registrierung über den Desktopcomputer an den Windows-Zertifikatserver weitergeleitet.
7. Die Zertifizierungsstelle sendet ein signiertes Zertifikat an den Desktop zurück, der dann das Zertifikat an das Gerät weiterleitet.
8. Das Gerät speichert das Zertifikat und dessen Zertifikatkette im Stammzertifizierungsstellenspeicher. Wenn sich das Stammzertifikat noch nicht im Stammzertifikatspeicher des Geräts befindet, werden Sie gefragt, ob Sie das Zertifikat akzeptieren möchten.
9. Am Ende der Registrierung wird ein Dialogfeld zum erfolgreichen Abschluss des Vorgangs angezeigt. Klicken Sie in **Get Device Certificate** (Gerätezertifikat abrufen) auf **OK** und dann auf **Schließen**.

Sobald sich das Zertifikat im Benutzerspeicher für Stammzertifikate oder Zertifizierungsstellen befindet, kann das Gerät mit dem gewünschten Protokoll authentifiziert werden.

Windows Mobile-Sicherheitsrichtlinien und Geräteprovisioning

In Ihrem Unternehmen sind Sie möglicherweise mit direkt erworbenen und mit indirekt erworbenen Geräten konfrontiert. Direkt erworbene Geräte sind diejenigen, die in großen Mengen direkt von einem OEM oder Mobilfunkbetreiber abgenommen wurden. In diesem Fall sind Sie vermutlich in der Lage, bestimmte Features anzufordern und mit dem Anbieter eine individuelle Gerätekonfiguration auszuarbeiten, die den Anforderungen Ihres Unternehmens entspricht. Indirekt erworbene Geräte sind diejenigen, die im Unternehmen durch einzelne Mitarbeiter oder Gruppen über einen Händler eingekauft wurden, oder die speziellen Anforderungen unterliegen, die einem direkten Erwerb entgegenstehen.

Die Herausforderung besteht in der gezielten Verwaltung der direkt und indirekt erworbenen Geräte. Diese Verwaltung erreichen Sie am besten durch eine fortlaufende Gerätekonfiguration, dem so genannten Provisioning, mit dem Sie die Sicherheitseinstellungen und sonstigen Features eines funktionsbereiten Geräts dynamisch ändern können.

Weitere Informationen zu den Sicherheitsfeatures von Windows Mobile-basierten Geräten und deren Interaktion mit Exchange ActiveSync finden Sie in den folgenden Whitepapers:

„Security Considerations for Windows Mobile Messaging in the Enterprise“ unter http://go.microsoft.com/fwlink/?LinkID=89638&clcid=0x409.

„Security Model for Windows Mobile 5.0 and Windows Mobile 6“ unter http://go.microsoft.com/fwlink/?LinkID=89639&clcid=0x409.

Sicherheitsrichtlinien und -rollen

Die Einstellungen der integrierten Sicherheitsrichtlinien von Windows Mobile-basierten Geräten definieren den Sicherheitsumfang. Beispielsweise bestimmen Sicherheitsrichtlinien, ob ein Gerät über ein Funknetzwerk (over-the-air, OTA) konfiguriert werden kann und ob es nicht signierte Nachrichten, Anwendungen oder Dateien akzeptiert. Die Einstellungen von Sicherheitsrichtlinien ermöglichen eine flexible Steuerung der Authentifizierung, der Datenverschlüsselung, von VPN (Virtual Private Networks), der Wi-Fi-Verschlüsselung und von SSL-Diensten. Diese Richtlinien werden global definiert und in ihren jeweiligen Komponenten in entscheidenden Bereichen der Gerätearchitektur lokal angewendet.

Sicherheitsrollen, wie z. B. **Manager** oder **Enterprise**, ermöglichen eine bessere Steuerung der Geräteressourcen und definieren, wer jeweils eine Richtlinie ändern kann. Die Rolle **Manager** ist in der Regel für den Gerätehersteller reserviert und ermöglicht eine vollständige Steuerung des Geräts. Diese Rolle dient dazu, die Geräte mit Einstellungen auszustatten und vorzukonfigurieren, bevor sie gekauft werden.

Mit einigen Berechtigungen der Rolle **Manager** auf dem Gerät können standardmäßig die meisten Sicherheitsrichtlinien geändert werden. Netzwerkadministratoren können mit der Rolle **Enterprise** Postfachrichtlinien in Exchange ActiveSync verwenden, um die Richtlinien zu ändern (siehe Neue Enterprise-Features in Windows Mobile 6 und Exchange Server 2007 in diesem Dokument). Wenn Sie vom OEM die Berechtigungen der Rolle **Manager** erhalten haben, können Sie außerdem alle Sicherheitseinstellungen des Geräts über das Provisioning ändern.

Provisioning von Mobile 6-basierten Geräten

Provisioning bezieht sich auf das Aktualisieren des Geräts nach der Herstellung und umfasst das Erstellen einer XML-Provisioningdatei. Diese Datei enthält Konfigurationsinformationen, die die Attribute von Features und Sicherheitsrichtlinien angeben. Die XML-Datei wird mit einem Zertifikat signiert und dann auf das Gerät übertragen. Hier konfiguriert der Konfigurationsdienstanbieter das Gerät anhand des Dateiinhalts.

Eine vollständige Provisioningdatei kann auf folgende Weise auf ein Windows Mobile-basiertes Gerät übertragen werden:

- OTA mithilfe eines OMA DM-Servers
- OTA mithilfe eines OMA Client Provisioning-Servers (ehemals WAP Client Provisioning)
- In eine CPF-Datei gepackt und mit Internet Explorer Mobile, ActiveSync, SI/SL oder eine Speicherkarte übertragen

Hinweis:

Führen Sie das Provisioning nach Möglichkeit mit OTA-Methoden aus. Wenn Sie die XML-Konfiguration in einer anderen Datei übertragen müssen, sollten Sie die Provisioningdokumente in ein CPF-Format (CAB Provisioning Format) packen und signieren. Ein XML-Provisioningdokument kann möglicherweise nicht auf einem Windows Mobile-basierten Gerät installiert werden, wenn die Datei mit den Dokumenten nicht signiert ist.

Hinweis:

CAB-Dateien und alle darin enthaltenen DLL- und EXE-Dateien müssen signiert sein, einschließlich reiner Ressourcen-DLLs.

Weitere Informationen zum Provisioning von Windows Mobile 6-basierten Geräten finden Sie auf der Homepage „Windows Mobile“ auf der MSDN®-Website unter http://www.microsoft.com/germany/msdn/mobile/default.mspx.

Schritt 7: Verwalten und Konfigurieren von Windows Mobile 6-basierten Geräten

Als Administrator stehen Ihnen mit Microsoft Exchange Server 2007 Tools zur Verfügung, mit denen Sie Sicherheitsrichtlinien für mobile Geräte festlegen und durchsetzen können. Außerdem können Sie einige der Features auf den mobilen Geräten mit den Provisioningtools steuern.

In diesem Thema finden Sie Anweisungen und Tipps zum Einrichten einer Verbindung zwischen mobilen Geräten und Exchange Server 2007 (unter Verwendung von Exchange ActiveSync).

Einrichten einer Verbindung zwischen mobilen Geräten und dem Exchange-Server

Wenn die Benutzer der mobilen Geräte einen Datennutzungsplan mit einem Mobilfunkbetreiber vereinbart haben, können E-Mail, Kontakte, Kalender und Aufgaben mithilfe von Exchange ActiveSync auf ihrem Gerät über ein Funknetzwerk synchronisiert werden. Alternativ können die Benutzer auch Desktop ActiveSync verwenden, um ihr Windows Mobile 6-basiertes Gerät mit einem Exchange-Server zu kombinieren. Dazu schließen sie das Gerät mit einem USB-Kabel an einem Desktopcomputer an, der mit dem Netzwerk verbunden ist.

Unabhängig von der Verbindungsmethode benötigen die Benutzer die folgenden Informationen von Ihnen, bevor sie ihre Geräte mit dem Exchange-Server synchronisieren können:

- Die Adresse des externen Mailservers.
- Exchange-Benutzernamen, Kennwort und die Domäne, die sie für den Zugriff auf den Exchange-Server benötigen.

Die Benutzer können mithilfe von ActiveSync auf ihren mobilen Geräten oder Computern auswählen, welche Art von Daten sie mit Exchange Server synchronisieren möchten, z. B. Kontakte, Kalender, Aufgaben der E-Mail. Raten Sie den Benutzern, die Datentypen zu deaktivieren, die nicht auf ihren mobilen Geräten gespeichert werden sollen.

Hinweis:

Weitere Informationen zu ActiveSync, einschließlich Schritt-für-Schritt-Anleitungen, finden Sie auf der Windows Mobile-Website unter http://go.microsoft.com/fwlink/?LinkId=37728 (möglicherweise in englischer Sprache).

Wenn die Benutzer sich für die Alternative mit Desktop ActiveSync entscheiden, raten Sie Ihnen, sicherzustellen, dass sie ihre mobilen Geräte direkt mit dem Exchange-Server synchronisieren. Die Direct Push-Technologie und Sicherheitsrichtlinien sind nur wirkungsvoll, wenn die Geräte direkt mit dem Exchange-Server synchronisiert werden. Das Synchronisieren der mobilen Geräte mit dem Desktopcomputer ist nicht empfehlenswert.

Herstellen einer Verbindung mit einem Exchange-Server mobil oder über ein Funknetzwerk

Die Benutzer der mobilen Geräte können Ihre Daten mithilfe von ActiveSync auf einem Windows Mobile 6-basierten Gerät direkt mit ihrem Exchange-Server synchronisieren.
Beim ersten Starten von ActiveSync auf ihren mobilen Geräten werden zwei Optionen angezeigt: das Synchronisieren der Daten mithilfe des Desktopcomputers und das direkte Synchronisieren der Daten. Wenn die Benutzer die Adresse ihres Exchange-Servers, ihren Exchange-Benutzernamen, das Kennwort und die Domäne kennen, erhalten sie vom ActiveSync-Assistenten die entsprechenden Anleitungen.

Bereitstellen von Windows Mobile 6-basierten Geräten mit Microsoft Exchange Server 2007

So verbinden Sie ein Windows Mobile 6-basiertes Gerät mit einem Exchange-Server:

1. Wählen Sie auf der Startseite **Start**, wählen Sie **Programs** (Programme), wählen Sie **ActiveSync**, wählen Sie **Menu** (Menü), und wählen Sie dann die Registerkarte **Configure Server** (Server konfigurieren). Wenn das mobile Gerät noch nicht mit Exchange Server synchronisiert wurde, ist die Option **Add Server Source** (Serverquelle hinzufügen) verfügbar.

2. Geben Sie unter **Edit Server Settings** (Servereinstellungen bearbeiten) den Namen des Exchange-Servers ein, und klicken Sie dann auf **Next** (Weiter).

3. Geben Sie Ihren Benutzernamen, das Kennwort und den Domänennamen ein, und wählen Sie dann **Next** (Weiter). Wenn das mobile Gerät Ihr Kennwort speichern soll, sodass Sie es beim nächsten Herstellen einer Verbindung mit Exchange nicht erneut eingeben müssen, aktivieren Sie das Kontrollkästchen **Save password** (Kennwort speichern).

4. Aktivieren Sie die Kontrollkästchen für die Informationselemente, die Sie mit Exchange Server synchronisieren möchten. Wenn Sie die verfügbaren Synchronisierungseinstellungen ändern möchten, wählen Sie die zu synchronisierenden Informationselemente aus, und wählen Sie dann **Settings** (Einstellungen).

5. Wählen Sie **Finish** (Fertig).